United States of America

Congressional Record

PROCEEDINGS AND DEBATES OF THE 112th CONGRESS, SECOND SESSION

Vol. 158 WASHINGTON, THURSDAY, JULY 26, 2012 No. 113

Senate

The Senate met at 9:30 a.m. and was called to order by the Honorable MICHAEL F. BENNET, a Senator from the State of Colorado.

PRAYER

The PRESIDING OFFICER. Today's guest Chaplain, Rev. John Fuller, senior pastor of Prairie Lakes Church in Cedar Falls, IA, will lead the Senate in prayer.

The guest Chaplain offered the following prayer:

Let us pray.

God of all nations and all peoples, we come before You on this day acknowledging You as the sovereign Lord of this Nation and of the whole world.

Father, it is a privilege to pray for these lawmakers, knowing that You hear and respond to the prayers of Your people. I pray for these women and men, whom You have put in this position, that they would be filled with Your wisdom to make wise choices and decisions as they lead this country. I pray that this body will be courageous, that they wouldn't be led by fear or their own personal desires but they would have the courage to lead with conviction that comes from You. Give these Senators strength to lead well through difficult times, that they would be strengthened in their inner being by a power that only comes from You.

And, Father, I pray for a spirit of humility that recognizes that others are more important than we are and that You have plans that are greater than ours; that, Father, we would lead with humble and gracious hearts.

We pray all this in Jesus's Name. Amen.

PLEDGE OF ALLEGIANCE

The Honorable MICHAEL F. BENNET led the Pledge of Allegiance, as follows:

I pledge allegiance to the Flag of the United States of America, and to the Republic for which it stands, one nation under God, indivisible, with liberty and justice for all.

APPOINTMENT OF ACTING PRESIDENT PRO TEMPORE

The PRESIDING OFFICER. The clerk will please read a communication to the Senate from the President pro tempore (Mr. INOUYE).

The assistant legislative clerk read the following letter:

U.S. SENATE,
PRESIDENT PRO TEMPORE,
Washington, DC, July 26, 2012.

To the Senate:

Under the provisions of rule I, paragraph 3, of the Standing Rules of the Senate, I hereby appoint the Honorable MICHAEL F. BENNET, a Senator from the State of Colorado, to perform the duties of the Chair.

DANIEL K. INOUYE,
President pro tempore.

Mr. BENNET thereupon assumed the chair as Acting President pro tempore.

RECOGNITION OF THE MAJORITY LEADER

The ACTING PRESIDENT pro tempore. The majority leader is recognized.

CYBERSECURITY ACT—MOTION TO PROCEED

Mr. REID. Mr. President, I now move to proceed to Calendar No. 470, S. 3414, which is the Cybersecurity Act.

The ACTING PRESIDENT pro tempore. The clerk will report.

The assistant legislative clerk read as follows:

Motion to proceed to Calendar No. 470, S. 3414, a bill to enhance the security and resiliency of the cyber and communications infrastructure of the United States.

Mr. REID. Mr. President, I would now yield to the senior Senator from the State of Iowa, Mr. GRASSLEY.

The ACTING PRESIDENT pro tempore. The Senator from Iowa.

PASTOR JOHN FULLER

Mr. GRASSLEY. Mr. President, it is my privilege to introduce Pastor John Fuller to my fellow Senators, and I thank Pastor Fuller for opening the Senate with prayer. It is my privilege to highlight my home pastor and church.

Pastor Fuller and his wife Kay are visiting the Nation's Capital this week.

Since 1998 Pastor Fuller has been the senior pastor at Prairie Lakes Church in Cedar Falls, IA. Pastor Fuller is a native of Iowa. He was born in Onawa and grew up in Sloan. His family moved to Sheridan, WY, when he was in the eighth grade. He graduated from high school in Sheridan. He played both high school and college football. He is to this day obviously a die-hard Broncos fan. You won't know that, but I sure know it. He is a 1986 graduate of the University of Sioux Falls and a 1990 graduate of Denver Seminary with a master's of divinity degree.

He was an associate and preaching pastor at First Baptist Church in Forest City, IA, before coming to Cedar Falls in 1998, to Prairie Lakes Church, and has been senior pastor. I have been worshipping at Prairie Lakes Church for 58 years come this August 29. The church has changed its name and increased its congregation over the years, but its heart has remained the same and very constant.

In 1855 a small group known as the Baptist Society started this church. In 1862 it became the First Baptist Church. The first 45 years that I worshipped at First Baptist Church, at various times the congregation numbered 200 to 300 people. Under Pastor Fuller's leadership, the number of worshipers has grown to about 2,000, with worship centers in Osage, Waterloo, and soon in Grennell, IA, besides the main campus in Cedar Falls, IA. In 2005 a new building was constructed, and the name of the congregation then became Prairie Lakes Church.

The worship service is very informal. That has changed in the 58 years I have attended there, but the service has always been Christ-centered, and that has not changed. Prairie Lakes Church

● This "bullet" symbol identifies statements or insertions which are not spoken by a Member of the Senate on the floor.

is multigenerational, with an extraordinary vision for the future. Worship services are heartfelt, creative, practical, Bible-based, and here to serve Christ and here to serve all—those who just stepped over the faith line as well as those who have been longtime followers of Jesus Christ.

Prairie Lakes Church is affiliated with the Baptist General Conference. Prairie Lakes Church is all about loving God, loving people, and influencing the world. Everyone is invited to worship with us—including anybody here in Washington, DC—through streaming online at prairielakeschurch.org.

In closing, I would remind all, according to the Scriptures, in Corinthians, we are all called to be ambassadors of Christ, and that is how I see Pastor Fuller.

I am also grateful to Pastor Fuller for his leadership and faithfulness to this congregation. After 58 years, in my looking back, I know God's word has been preached faithfully at this congregation. Pastor Fuller has contributed significantly during his tenure and continues to do so.

This is what Pastor Fuller had to say about our church:

> There are a lot of good churches around the valley. We're lucky to have that. I think people get attracted here because we just stick with the Bible. We're authentic. We're invitational, and we try to keep things simple.

These attributes have attracted many, and I believe they will continue to attract many more and the church will continue to grow.

Lastly, I pray that God will continue to shine His light through Pastor Fuller, his family, and the Prairie Lakes congregation. It is my privilege once again to introduce Pastor Fuller to this Senate.

I yield the floor.

The ACTING PRESIDENT pro tempore. The majority leader.

Mr. REID. Mr. President, I appreciate my friend's remarks about his pastor. They were very well thought out, and I appreciate them very much.

SCHEDULE

Mr. REID. Mr. President, the first hour here today will be equally divided and controlled between the two leaders or their designees. The majority will control the first half and the Republicans the final half.

I filed cloture last night on a motion to proceed to the cybersecurity bill. I hope we can reach an agreement to have that cloture vote sometime today. If not, we will have it tomorrow.

When a major storm ripped through the Mid-Atlantic region last month, it left millions of people without power—I repeat, millions of people. I was at my home here in Washington, which is different from my home in Searchlight, NV. In Searchlight, the wind blows a lot, so you can hear the wind. It is kind of pleasant for me. But the wind we heard at our home in Washington was not pleasant. At 9:30 or 10:00 at night, it was loud and it was abusive and it was, quite frankly, a little scary.

Our power was not affected, but that wasn't the case for millions of other people. Residents of Maryland, Virginia, West Virginia, Ohio, and the District of Columbia soon realized how quickly a major power outage can alter life as we know it. I talked to Senator MANCHIN of West Virginia, and a week later power was still out in large parts of West Virginia. He said it was the worst storm they have ever known in West Virginia.

This power outage altered life as people knew it here in the entire eastern part of the United States. The blackout was devastating to many families and many businesses. But it was also minor compared to the devastation that malicious cyber terrorists could wreak with a single keystroke. I repeat, as damaging and frightening as this storm was, we could have a malicious cyber attack by terrorists that would be far more devastating than this violent storm. Cyber attackers could all too easily shut down the electric grid for the entire east coast, the west coast, and the middle part of our country. Any one attack could leave dozens of major cities and tens of millions of Americans without power. We know, because we were shown in a room here in the Capitol, how an attack could take place and what damage it would do, so we know this is not just make-believe.

Without ATMs or debit card readers, commerce would immediately grind to a halt. My daughter, who lives here in the DC area, lost power when the storm hit. They waited for a number of hours, and then they took all the food out of their freezer, they gave away what they could, and they threw the rest away. And that was the way it was all over. Their power was out for about a week, and it made it very difficult. They are fortunate enough to have a basement, and the heat wasn't oppressive down there.

Without refrigeration, food would rot on the shelves, the freezers would have to be emptied, and people could actually go hungry. Without gas pumps, transportation arteries would clog with abandoned vehicles. Without cell phones or computers, whole regions of the country would be cut off from communication and families would be unable to reach each other. Without air-conditioning and without lifesaving technology and the service of hospitals and nursing homes, the elderly and sick would become much sicker and die. Most major hospitals have backup power, but it is only for a limited amount of time. It depends on how much fuel they can store, and that is very limited.

The devastation is really unimaginable, but we have heard these ominous scenarios before. What many Americans haven't considered is that the same power grids that supply cities and towns, stores and gas stations, cell towers and heart monitors also power every military base in our country. About 99 percent of electricity used to power military installations comes from outside the bases. Nellis Air Force Base, one of the largest in the world of its type, has some solar energy there that they have developed, but over 90 percent of their power, in spite of that, comes from outside the base, and more than 85 percent of that power is provided by the same electric utilities that power homes and businesses and schools in the civilian world. So a cyber attack that took out a civilian power grid would also soon cripple our Nation's military—very soon.

Although bases would be prepared to weather a short power outage with backup diesel generators, within hours, not days, fuel supplies would run out. Command and control centers would go dark. Radar systems that detect air threats to our country would shut down. Communication between commanders and their troops would go silent. And many weapons systems would be left without either fuel or electric power.

Much of what we do militarily is now done by computers and done very remotely. It is no secret that the drones that operate for our country all over the world are not operated from Pakistan, Afghanistan, or Somalia, they are operated from a base 35 miles outside Las Vegas. That is all done with electricity. So in a few short hours or days, the mightiest military in the world would be left scrambling to maintain base functions.

That is why our top national security officials—including the Chairman of the Joint Chiefs, the Director of the National Security Agency, the Secretary of Defense, and the CIA Director—have said that the kind of malicious cyber attack I have just described is among the most urgent threats to our country. In fact, they have said that unless we do something and do it soon, it is not a question of if, it is only a question of when.

There have already been cyber attacks on our nuclear infrastructure, our Defense Department's most advanced weapons, the NASDAQ stock exchange, and most major corporations. These are just a few of the things that have already been attacked by cyber.

Senator MCCONNELL and I recently received a letter from a bipartisan group of former national security officials, including six former Bush and Obama administration officials, that presented the danger in stark terms:

> We carry the burden of knowing that 9/11 might have been averted with the intelligence that existed at the time. We do not want to be in the same position again when ''cyber 9/11'' hits—it is not a question of whether this will happen; it is only a question of ''when.''

That is what they said, not me. The group said the threat of cyber attack ''represents the most serious challenge to our national security since the onset of the nuclear age sixty years ago.''

The bill before this body, proposed by a coalition of Democrats and Republicans—including Chairman LIEBERMAN

and ranking member COLLINS—is an excellent piece of legislation endorsed by many members of the national security community.

In my view, it is not strong enough, but it is a tremendous step forward, and I admire the work they have done. I know some of my colleagues have suggestions on how to improve this legislation. I have a few of my own. There is plenty of room for good ideas. Some of them are already on the table. It is my intention for Senators to have an opportunity to have a robust debate on these proposals. Let's stick with what this bill is all about and let's have as many amendments as people feel is appropriate.

The national security experts agree we can't afford to waste more time. The question is not whether we should act but whether we will act in time.

As I mentioned at the start, we are scheduled to have this vote an hour after we come in tomorrow. I am working with Senator MCCONNELL now to try to arrange a time, perhaps even today. My goal is to get on the bill. I hope we can get on the bill. It would be terrible for our country if we are not on the bill. I would like to get on the bill and have Senators LIEBERMAN, COLLINS, ROCKEFELLER, FEINSTEIN, and the other committees that are involved come up with a list of amendments as we have done so well on a number of the bills we have worked through. When we come back next week, let's start doing some legislating and have some robust debate, get some of these amendments disposed of, and pass this bill on to the House.

The House has done their bill. We can go to conference and get something done. It would be very important for our country.

RECOGNITION OF THE MINORITY LEADER

The ACTING PRESIDENT pro tempore. The Republican leader is recognized.

THE ECONOMY

Mr. MCCONNELL. Mr. President, yesterday our Democratic friends took a vote that says a lot about the way they view the world. After nearly 4 years of spending and debt, millions of Americans are still struggling amidst the slowest recovery in modern times, and the economy is flat on its back. Our friends on the other side think a great way to go forward is to raise taxes. Under the guise of pretending to care about the deficit, Democrats are pushing an ideological goal of a symbolic tax increase that would not even fund the government for 1 week. The vote we had yesterday—with all but two of the Democrats on board—allegedly doing something about the deficit wouldn't fund government for 1 week.

They are not even pretending to care about the economy. They have sort of given up on the argument that this is about the economy. We know that because 2 years ago the Democrats agreed the higher taxes they are now fighting for would hurt the economy.

Let's look at the economy then and the economy now. At a time when economic growth was 3½ percent, back in December of 2010, 40 Democrats voted to keep rates where they were on the grounds that it was the best thing to do for jobs. In December 2010, 40 Democrats voted to keep the tax rates where they were because it was the best thing for jobs. Yet now when the growth rate is 2 percent—it was 3½ percent then, it is 2 percent now—and 13 million Americans are still out of work, they are voting to slam nearly 1 million businesses with a tax increase. Maybe they are expecting the GDP numbers tomorrow to be 3½ percent. We will see.

That is one of two things, either our Democratic friends don't even care about the economy and jobs anymore and are just embracing Thelma-and-Louise economics—let's take everybody off the cliff and hope people support them for some other reason—or their economic world view is so far outside the mainstream of everyone else who has looked at the situation that they think 2 percent growth and 13 million Americans unemployed is good enough. Maybe they think that is as good as we can do. That is where this ideological crusade of theirs is taking them, right in that direction. I just hope for the sake of a struggling American economy that some of them soon see how misguided an approach this is.

Let me repeat, 2 years ago in December of 2010, when the economy was growing at a rate of 3½ percent, 40 of our Democratic colleagues, the President, the Vice President, me, and the Speaker agreed to extend the current tax rates for 2 years because it would be good for jobs.

Just yesterday, with two exceptions, every Democrat voted to raise taxes on 1 million businesses when the growth rate—the GDP increased rate—is 2 percent and 13 million Americans are looking for work. That is not a prescription for the economy; that is an ideological crusade. That is not about America's jobs; that is about the election 4 months from now.

I yield the floor.

RESERVATION OF LEADER TIME

The PRESIDING OFFICER (Mr. MANCHIN). Under the previous order, the leadership time is reserved.

ORDER OF BUSINESS

Under the previous order, the following hour will be equally divided and controlled between the two leaders or their designees, with the majority controlling the first half and the Republicans controlling the final half.

The Senator from Colorado.

PRODUCTION TAX CREDIT

Mr. UDALL of Colorado. Mr. President, I rise to speak on the floor of the Senate again this morning to urge my colleagues to vote to extend the production tax credit for wind energy. It is also known as the production tax credit. I know the Presiding Officer's home State of West Virginia has a robust wind energy sector as well. I look forward to coming to the floor and talking about the Presiding Officer's State in the future.

The reason I am talking about the production tax credit is it is set to expire at the end of this year, and it will cost citizens in my State and the rest of the Nation their jobs. We cannot let this happen. Tens of thousands of vital jobs are dependent on the wind industry all across our great country.

As I have mentioned, I come to the Senate floor on a daily basis and I highlight a State and talk about what the production tax credit has done to encourage economic growth in that State. Today, I wish to talk about the great State of Illinois, the land of Lincoln, where the wind industry is thriving. Illinois is an impressive example of how wind resources can be harnessed and put to good use creating jobs and supporting local communities.

Overall, Illinois has the fourth largest installed wind capacity in the United States, with over 600,000 homes powered by the wind. If fully utilized, the wind energy resource in Illinois could provide 525 percent of the State's current electricity needs. That is truly a staggering amount of electricity for the fifth largest State in the Nation.

In 2011, Illinois was second only to California in the number of new wind energy projects completed, and they installed more wind turbines there than any other State in the country. Clearly, Illinois recognizes the economic potential wind energy holds for the future, as many other States have.

Just last week in Illinois, Invenergy announced it completed construction of the Bishop Hill wind energy facility in Henry County. That is up in the northwestern part of Illinois, near Davenport, IA. The project covers 22,000 acres of farmland and includes over 100 wind turbines and can power 60,000 homes. The Bishop Hill project is clearly a huge investment in Illinois and our Nation's clean energy future. But the economic power of wind energy has been equally impressive. The wind energy there supports 7,000 jobs, it contributes close to $19 million every year in property taxes to local communities, and Illinois led our Nation in 2011 with over 400 new wind turbines installed.

Just this month, Illinois State University released a report that estimates that the 23 largest wind farms in Illinois will contribute roughly $5.8 billion to the local economies over the lifetime of these projects. The construction of these wind farms generated over 19,000 jobs that cut paychecks totaling over $1 billion for workers. These are good-paying, high-skill jobs that we are proud to have in our country and that American workers are proud to have and it is one part of the overall wind energy story.

For example, the Odell Grade School, in Odell, IL, has a much needed project underway that will expand the school and make it more energy efficient. While this project is expensive, it will be paid for, in part, by payments from local wind farms. Wind energy is supporting a better education for Odell's youth without increasing taxes to the local residents.

This is not unique to Illinois. It is happening all across our country. I have no doubt the people of Odell would agree with me that extending the PTC is a commonsense proposal. However, without Congress extending the production tax credit, our country and the wind industry literally face impending disaster. In fact, many wind energy manufacturers and producers have already been preparing for the end of the PTC by backing off their investments in many of these communities such as Odell and by announcing future layoffs of thousands of workers. It is just flatout unacceptable that we in the Congress would let this happen.

I think everyone understands where I am heading. This is a serious issue that needs attention now—not next month, not in the fall, not in the lameduck session but now. The wind industry will not wait for us to extend the PTC at some date in the future. They have already begun to scale back their operations and move overseas. Further inaction is unacceptable. China is stepping into the breach and literally taking our jobs overseas. Other countries are prepared to do the same. For us in Congress to miss this opportunity to not only preserve jobs but put in place policy that would create thousands of good-paying jobs because of election-year gridlock is flatout unacceptable. If we don't act, our people in our States will suffer.

I come to the floor every day to implore my colleagues to extend the wind production tax credit as soon as possible. The PTC equals jobs. We ought to pass it as soon as possible. I will be back next week to continue discussing the wind Production Tax Credit and urge us to be bold, take up this issue and extend the wind production tax credit. It is about American jobs. It is about maintaining our leading position in the world when it comes to clean energy development.

I yield the floor and note the absence of a quorum.

Mrs. MURRAY. If the Senator could abstain from the quorum, please.

The PRESIDING OFFICER. Without objection, it is so ordered.

The Senator from Washington.

VIOLENCE AGAINST WOMEN ACT

Mrs. MURRAY. Mr. President, I come to the Senate floor today in order to continue the efforts started right here earlier this week, efforts by the women of the Senate and the men who support the Violence Against Women Act to bring a simple, straightforward message to our friends in the House of Representatives: Stop the games and pass the inclusive, bipartisan Senate VAWA bill without delay.

The Violence Against Women Act is a bill that has successfully helped provide lifesaving assistance to hundreds of thousands of women and families. It is a bill that passed the Senate 3 months ago today by a vote of 68 to 31. It is a bill that has consistently included bipartisan provisions to address those who are not being protected by it each and every time it has been reauthorized. But here we are, back on the Senate floor, urging support for a bill that should not be controversial.

Just as we did on Tuesday, just as we are doing today, and just as we are going to continue to do in the coming weeks, we will be making sure this message resonates loudly and clearly both in Washington, DC, and back in our home States because we are not going to back down—not while there are thousands of women across our country who are excluded from the current law. In fact, for Native and immigrant women and LGBT individuals, every moment our inclusive legislation to reauthorize the Violence Against Women Act is delayed is another moment they are left without the resources and protection they deserve in this country.

The numbers are staggering: 1 in 3 Native American women will be raped in their lifetimes—1 in 3. And 2 in 5 of them are victims of domestic violence, and they are killed at 10 times the rate of the national average. These shocking statistics are not isolated to one group of women; 25 to 35 percent of women in the LGBT community experience domestic violence in their relationships, and 3 in 4 abused immigrant women never enter the process to obtain legal status, even though they were eligible, because their abuser husbands never filed their paperwork.

This should make it perfectly clear to our colleagues in the other Chamber that their current inaction has a real impact on the lives of women across America affected by violence, women such as Deborah Parker. Deborah is the vice chairman of the Tulalip Tribe in my home State of Washington.

Deborah was repeatedly abused starting at a very young age by a nontribal man who lived on a reservation. Not until after the abuse stopped—sometime around when she was in the fourth grade—did Deborah realize she was not the only child suffering at the hands of that same assailant. At least a dozen other young girls had fallen victim to that man—a man who was never arrested for his crimes, never brought to justice, and still walks free today, all because he committed these heinous acts on the reservation. As someone who is not a member of a tribe, it is an unfortunate reality that he is unlikely to ever be held liable for his crimes.

Reauthorizing an inclusive VAWA is a matter of fairness. Deborah's experience and the experience of other victims of that man do not represent an isolated incident. For the narrow set of domestic violence crimes laid out in VAWA, tribal governments should be able to hold accountable defendants who have a strong tie to the tribal community.

I was very glad to see Republican Congresswoman JUDY BIGGERT and several of her Republican colleagues echo those sentiments last week. They sent a letter to Speaker BOEHNER and Leader CANTOR. These Republican Members explicitly called on their party leadership to end this gridlock and accept the ''Senate-endorsed provisions that would protect all victims of domestic violence, including college students, LGBT individuals, Native Americans and immigrants.''

So today I am here to urge Speaker BOEHNER to listen to the members of his own caucus and join us in taking a major step to uphold our government's promise to protect its people, people such as Maribel and Maria, two more constituents who come from my home State of Washington.

As a transgender woman, Maribel has been subject to random acts of violence by family and boyfriends and strangers. She has been mugged and attacked on the street. She has suffered broken bones and cuts and bruises. She has been raped, and she was left for dead. What Maribel said to me was deeply concerning. She said:

> Not once have the police ever conducted an investigation, much less shown any concern for me. Rather my experience with law enforcement is one of harassment and abuse. I have been ostracized by family and friends . . . in fact it is most of my first memories.

She experiences hate daily from those who think she has no place in our society.

Then there is Maria. Shortly after their wedding, Maria's husband became a different man, she said. His abuse ranged from emotional to physical, and on two separate occasions he held a knife to Maria's throat threatening to kill her. He constantly threatened Maria with deportation back to Jamaica. Eventually, he refused to attend the interview with immigration authorities necessary for her to obtain a green card. Her application was denied for lack of attendance. She was angry and scared, but she found the courage to ask her husband for a divorce. In response, he raped her. Maria moved out of the house though her husband repeatedly tracked her down and assaulted her. To save her own life, Maria fled to Seattle with her two young children.

It does not have to be this way. I was so proud to have been serving in the Senate in 1994 when we first passed the Violence Against Women Act. Since we took that historic step, VAWA has been a great success in coordinating victims' advocates and social service providers, and law enforcement professionals to meet the immediate challenges of combating domestic violence. Along with its bipartisan support, it has received praise from law enforcement officers and prosecutors, judges, victim service providers, faith leaders, health care professionals, advocates, and survivors.

The Violence Against Women Act has broad support for one reason: It works. Where a person lives, their immigration status, who they love should not determine whether perpetrators of domestic violence are brought to justice. These women cannot afford any further delay—not on this bill.

Mr. WYDEN. Mr. President, would the Senator yield for a question.

Mrs. MURRAY. I would be happy to yield for a question.

Mr. WYDEN. I think the Senator from Washington has made an extraordinary presentation in terms of outlining the facts of the abuse women face. Having done a series of forums around my home State—as my colleague knows, in our part of the country in Washington and in Oregon where there are many small communities of 10,000, 15,000 people, it is my experience—and I would be interested in getting the assessment of our colleague since she has been a leader on this—that without the Violence Against Women Act, it is my understanding that women in rural areas who face the kind of brutal treatment my colleague described would literally have nowhere to turn, so that the Violence Against Women Act for women in rural areas in particular is sort of the last line of defense for them.

Mrs. MURRAY. The Senator from Oregon is absolutely correct. If a woman has been beaten and abused and believes she is a victim of violence with nowhere to turn, especially in a rural community where everyone knows everyone and a person doesn't know who to turn to, there is no place to go. The Violence Against Women Act provides the support of law enforcement officers and advocates so a person can get out of a very abusive situation.

Mr. WYDEN. I am going to listen to the rest of my colleague's remarks, and I will have my own. But I just want to thank the Senator from Washington for her leadership. This is such an important issue. It is not about dollars and cents, and it is not about politics. It is about doing what is right for combating violence, and I commend my colleague.

Mrs. MURRAY. I thank my colleague from Oregon. I know he is going to speak in just a few minutes, but I know he has spent a great deal of time traveling around his State and listening to these women and he knows personally from their stories how important it is that we cannot continue to delay this bill over something called a blue slip. It is not about a blue slip. It is about doing what is right.

We have overcome the blue slip issue time and time again for issues such as FAA and Transportation bills and many other pieces of legislation because it is the will of the body to do so. So to tell a woman in Oregon or Washington State that this bill can't happen because of a blue slip is ridiculous. They have been told they can't get help for a lot tougher reasons. Let's not let a blue slip be what comes between them and the support they need.

In fact, I say to my colleague from Oregon and all of my colleagues that on Tuesday the New York Times ran an editorial that gets to the heart of it. They said:

House Republicans have to decide which is more important: Protecting victims of domestic violence or advancing the harsh antigay and anti-immigrant sentiments of some on their party's far right. At the moment, harshness is winning.

The editorial also echoed our sentiments that it does not have to be this way. It pointed out:

In May, 15 Senate Republicans joined with the chamber's Democratic majority to approve a strong reauthorization bill.

It ends with what we all know it will take to move this legislation forward: leadership from Congressman BOEHNER. So today we are on the Senate floor to make this effort and to call for the same thing: leadership.

It is time for Speaker BOEHNER to look past ideology and partisan politics. It is time for him to hear the stories of women across America who have not had the protection of this bill and to make a major step forward which will assure that a woman, no matter where she lives or who she is, will have the protections this great country can offer.

So I thank my colleague from Oregon for his real passion and understanding on this issue and for taking the time to hear from women and men who have been impacted.

I yield the floor.

The PRESIDING OFFICER. The Senator from Oregon.

Mr. WYDEN. Mr. President, I wish to follow on the very important remarks made by our colleague, Senator MURRAY. As a result of the debate we have had in Washington, DC, I knew there was a significant problem, but until we held these forums across our State—we essentially went into every corner of Oregon—it really didn't come home to me how serious a problem this is.

I wish to highlight for a moment or two this point I got into with Senator MURRAY with respect to rural areas, some of the stories. For example, I was told about a woman in central Oregon who essentially, faced with a very abusive relationship, spent the evening trying to hide out in ditches in the community. She would just run from ditch to ditch. Of course, a person gets pretty banged up and bruised when they do something like that, but she hid out in ditches through the night in order to avoid her abuser.

But then it came to morning time and she wanted to get out. She wanted to get to the Safety Net program, which is a wonderful shelter in her area. But the fact was the only way to get out was to ask for a ride from the one person who had a vehicle in the community, and that was the person who abused her in the first place. So, literally, in a rural community—and I heard this account just recently—she had nowhere to turn. That is why I characterize the Violence Against Women Act as—especially for rural women—the last line of defense between them and the abuser.

In another community—I know my colleague, the Presiding Officer, will identify with this, and I enjoyed going to West Virginia and the like—in a rural community in the eastern part of our State, it was described to me that there was no transportation out of the community. There was no transportation at all. The woman involved was going to literally have to stay there and face continual abuse. The one vehicle in the community was a fishing shuttle.

I am sure the Senator from West Virginia identifies with that. It is something we have in our rural communities—a vehicle that takes folks fishing.

The owner of the fishing shuttle said: I am going to be the one to take this woman to safety. I don't need to be reimbursed. I don't need to have some kind of government program or something. I am going to do it because it is right.

That is how that woman in a rural community escaped her abuser. She got out. She got free. She was able to shake out of the clutches of the abuser because the fellow who owned the fishing shuttle stuck up for her.

But I think this is Senator MURRAY's point: I do not think we can accept that all across the country we are going to have fishing shuttles available in order to rescue women who are subject to this kind of abuse. I think that is pretty farfetched, and the good hearts of Oregonians came through in that particular situation, but we have to reenact this program.

The fact is, Mr. President and colleagues, this has been the law of the land for more than a decade. There has not been a shred of partisanship in it. It is not about ideology. It is about protecting women from brutality. I had thought, frankly, we had gotten over some of the arguments against this legislation that had been trotted out in the past.

For example, it was often said in the past: Well, maybe these abuse cases are not abuse. Maybe they are just kind of family matters. They are going to get settled when the family kind of calms down. Maybe somebody got upset about something, and then in a day or so everything is going to go back to normal.

That is not the case. This is about repeated instances of violence, repeated instances of violence you cannot slough off as a family difference of opinion. It is a crime. It is brutal violence. That is why we need this legislation, and we need it reauthorized.

I think it is also especially important, given some of the budget cuts we have seen that are particularly hitting small communities like a wrecking ball. For example, in Josephine County—a rural part of our State—they are in the position where, when a subpoena goes out, they essentially do not have the resources to follow it up. In other words, the subpoena is used to, in effect, set in motion the law enforcement process to bring the abuser to justice, and I was told by the key law enforcement officials in Josephine County—in a community forum I held in Medford, OR, for folks from the southwestern

part of the State—that they literally do not have the resources to follow up on how to ensure that abuser is brought to justice.

I would make a couple of additional points. I see colleagues on the floor waiting to speak.

I also want to talk about the costs that are associated with this. You have two kinds of costs. First, you have direct health care costs that stem from the violence you see perpetrated against women, and then also you have costs in terms of lost productivity. At a time when we are getting hit very hard by unemployment—and we know we are in a productivity race with Asia and India and China and other countries—we cannot afford the costs, the health care costs of the violence against women that ends up having women land in hospital emergency rooms and the like, nor can we allow this lost productivity at a time when we are pushing so hard to create more good-paying jobs.

The protection that is offered through the Violence Against Women Act saves my home State of Oregon now millions of dollars through its key provisions. Safety from domestic violence would save Oregon more than $35 million per year in direct health care costs. Our State loses approximately $9.3 million per year in lost productivity from paid work as a result of domestic violence. The fact is, the preventive services offered by the Violence Against Women Act saves money, as does the very important work that is done by victim services.

The study of 278 victims in my home town of Portland who received domestic violence and housing assistance found that those services resulted in more than $610,000 in savings during the first 6 months. So there are savings in terms of assistance, whether it is housing or counseling. Emergency medical care utilization is reduced as a result of emergency services, safety net services being available. Whether it is one measure or another, from a financial standpoint, reauthorizing the violence against women legislation makes sense.

But at the end of the day, while the financial savings are substantial, it seems to me the Violence Against Women Act is about restoring dignity to women who have been abused in our country. No woman in the United States should be subject to the kind of physical abuse I have documented in cases coming from Oregon and that Senator MURRAY has described this morning. They strip our people—women in this country—of their dignity and their confidence and their ability, after they shake free from their abuser, to get on and have the kind of productive life they want for themselves and their family.

Ultimately, this is about dignity. It is about doing what is right. This legislation has been on the books for more than a decade. There is no reason—none whatever—that this legislation is not passed overwhelmingly on a bipartisan, bicameral basis. I am going to do everything I can here on the floor of the Senate talking with colleagues on both sides of the aisle to make sure this legislation is reauthorized. Because what I saw during these community forums in my home State, from small towns across Oregon, should not happen in my State, it should not happen anywhere, because it is not right, and the Senate can take action to stop it.

With that, I yield the floor.

The PRESIDING OFFICER. The Senator from Arkansas.

PASSING APPROPRIATIONS BILLS

Mr. BOOZMAN. Mr. President, there has been a lot of talk about the dangers of raising taxes during a recession. President Obama famously said in 2009: ''You don't raise taxes in a recession.'' Our economy is certainly worse now than it was then. But that did not stop the Senate majority from pushing through a tax increase on our small business owners yesterday.

We need to get our fiscal house in order, and that starts with budgeting in a responsible manner. Washington's primary problem is not a revenue problem. Washington's primary problem is a spending problem, and the Senate majority's actions have exacerbated that problem.

The Senate has failed to pass a budget for the past 3 years. Meanwhile, our country is facing record deficits and an ever-increasing debt. This is the fifth straight year that Washington's excessive spending has led to a trillion-dollar deficit. It now sits at a jaw-dropping $15.9 trillion. The Senate majority's only answer to this crisis is to raise taxes on our job creators during a time while our country has an unemployment rate of over 8 percent.

Along with failing to produce a budget, the Senate majority leader is now backtracking on a pledge to enact every individual appropriations bill this year. Needless to say, I am disappointed. In fact, I think it is safe to say our entire caucus is disappointed.

It was not too long ago that I was down here on the floor praising the majority leader in his efforts and those who would have us go forward and enact our individual appropriations bills. We believed we had a good-faith agreement to move these bills, to make the effort to function the way this body was established to work, to do our job and pass all of the appropriations bills so that the government operates on a budget the way every Arkansan does.

Now the majority is telling us this is not going to happen. Determining how we spend hard-earned taxpayer dollars is a basic responsibility of Congress. We know tough choices have to be made in these appropriations bills, but moving forward is the right direction. The trend of continuing resolutions and giant omnibus appropriations bills has to stop.

Enacting all appropriations bills in regular order would be an important step to reducing government spending. It would help balance our budget while investing in programs Americans have come to rely on.

Moving forward on these bills would return the Senate to its proper function and provide a framework of spending so the American people can see and understand where their hard-earned money is going. Most importantly, it would help us back away from the fiscal cliff we are hanging on to.

Here is the reality: We borrow around 40 cents of every $1 we spend. We are running record-breaking deficits every year. The average American family does not have the luxury to live by this sort of budgeting. If you tried to run your household, your business this way, the bank would cut you off. It is time we apply that lesson to Washington.

We are at a crossroads in our country. If we continue down the path we are going, we risk going in the direction of Greece, Ireland, Portugal, and now Spain—each facing economic crises that have pushed them to the brink of default.

If Congress continues the reckless spending, rather than crafting an immediate solution to this crisis, our actions will inevitably lead to an economic collapse. We cannot keep kicking the can down the road, which is exactly what we are doing by passing continuing resolutions and omnibuses after continuing resolutions and omnibuses. It goes on and on.

Each one of us in this Chamber owes it to the American people to work together to help our country today and build a path of success for the future. Our Founding Fathers laid the foundation that allows the Senate to function effectively and efficiently, but it does require us working together.

The American people are tired of the finger pointing that has stalled much of the work they have sent us here to do. That starts with trying to enact all of the appropriations bills through a regular process each year. I sincerely hope the Senate majority leader reconsiders the decision to cancel consideration of the appropriations bills, again, so we can get back to a normal budgeting process, get back to a normal method, an efficient method, a very transparent method, so the American people can see where their taxpayer dollars are going.

With that, I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

The PRESIDING OFFICER (Mr. UDALL of New Mexico). The Senator from Oklahoma is recognized.

Mr. COBURN. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. COBURN. Mr. President, I assume we are out of morning business.

The PRESIDING OFFICER. The Senate is on the motion to proceed to S. 3414.

UNANIMOUS CONSENT REQUEST—S. 3326

Mr. COBURN. Mr. President, I have a unanimous consent request.

I ask unanimous consent that the Senate proceed to the immediate consideration of S. 3326; that the Coburn amendment at the desk be agreed to, the bill, as amended, be read a third time and passed; that when the Senate receives the House companion bill to S. 3326, as determined by the majority and the Republican leaders, the Senate proceed to its immediate consideration; that all after the enacting clause be stricken, and the text of S. 3326, as passed by the Senate, be inserted in lieu thereof; that the bill be read a third time and passed; that a statutory pay-go statement be read, if needed, and passed with no amendments in order prior to passage, the motions to reconsider be considered made and laid upon the table with no intervening action or debate, and any statements related to the bill be printed in the RECORD at the appropriate place, as if read.

The PRESIDING OFFICER. Is there objection?

The Senator from Montana.

Mr. BAUCUS. Mr. President, I reserve the right to object and would like to make a statement.

I am basically opposed to the Senator's request, and let me explain why. The Finance Committee considered this bill last week, and we passed it out of committee by a voice vote without a single amendment being offered. Nobody on the committee offered an amendment. I think we cannot and should not delay the passage now. It passed unanimously, no amendments offered, and now is not the time to delay.

This bill is fully offset. How? By extending customs user fees and corporate timing shift. This is not the first time we have used the corporate timing shift as an offset. I have a list—a very long list—of the many times when this body has used this very same provision and very same offset. In fact, it has been used multiple times since 2005 in trade bills and lots of other bills, so there is much precedent.

I, nonetheless, understand Senator COBURN now has concerns about the offset, and I am willing to work with him to find alternate offsets in future trade measures. We need to move forward on this bill in its entirety as soon as possible. We can't pick and choose to move forward on component parts while leaving others to linger. There are real consequences for delay.

This bill extends provisions of the African Growth and Opportunity Act—otherwise known as AGOA—trade preference program that would otherwise expire in September. Without swift passage of this bill, U.S. retailers do not have the certainty they need to place orders with African apparel manufacturers. Not only are these U.S. companies struggling to make the best decisions for their companies, but a substantial drop in orders has caused devastating job losses in Africa. The job losses are occurring why? Because of the uncertainty as to whether this provision will be extended. Right now the Senator from Oklahoma suggests we don't proceed.

Another provision of this bill closes a loophole in the Dominican Republic-Central American-United States Free Trade Agreement that will save almost 2,000 yarn-spinning jobs in North Carolina and in South Carolina. And the Burma sanctions provision expires today. These provisions are all necessary parts of the delicate compromise we negotiated in advance with the House and that the Senate Finance Committee approved. Ways and Means Chairman CAMP in the House and Ranking Member LEVIN in the House have made it equally clear they will not pass this bill in the House without the AGOA provisions included. So the House will not pass these provisions if the Senator is successful.

I, therefore, urge my colleagues to pass S. 3326 as it passed from the Finance Committee, quickly and without amendment. For those reasons, I must object.

The PRESIDING OFFICER. Objection is heard.

The Senator from Oklahoma.

Mr. COBURN. Mr. President, short memories are just that. In my opening statement in the Finance Committee on this bill, I made it very clear I opposed the pay-for in this bill. I had two amendments to offer. They were not offered because the chairman had assured me beforehand that he would object and rule them nongermane, even though they were not nongermane. As a matter of fact, we had offered what the Obama administration had already offered in terms of trade duplication—a $200 million pay-for that the administration supports.

So let's talk about what is really going on here. We are a country that is $15.8 trillion in debt. We have a process that is not open, really, to the consideration of addressing real pay-fors for a real bill that I agree needs to pass. I have no objection to the underlying policies in any of the three components in this bill, but there is a process we continue to practice which has our country bankrupt. That process is the following: We are going to spend $200 million over the next 3 years, and then we are going to take 10 years to pay for it.

We have $350 billion in waste, fraud, and duplication in the Federal Government that we have done nothing about as a Senate. Not one thing have we done to address the issues that are wasting the hard-earned money of the taxpayers of this country. So when we have a small bill and administration concurrence on something that should be eliminated, and yet we would rather not do that but just kick the can down the road, we are failing the American people.

I have a great deal of respect for the chairman of our committee, but it seems to me that my conversations with the Speaker and Mr. CANTOR and Mr. CAMP in the House are much different than his. As a matter of fact, if we were to divide this, they would divide theirs and pass them both back over here, and we could do the same. What I have offered is to separate out these two from the AGOA package. I am for that. I just think we ought to pay for it.

What I have offered, and I offer to do now if the chairman splits it, is to have 30 minutes on the floor to explain why I want to pay for the AGOA, then have a vote, and let it go. But we will not even do that. So not only do we not want to address the problems, we don't even want to have a debate and an opportunity to stand up and say whether we are for cutting wasteful spending, which even the administration is for. That is what is offered.

So now we stand here, with Burma sanctions going to expire. I am going to tell you, I am not moving. I will object to any unanimous consent request that doesn't have a real pay-for for the $200 million for this bill out of real spending in the next 1 or 2 or 3 years, which is exactly what we offered to put forward in committee and what we have offered to negotiate. I am not going to be a part of kicking the can down the road again. I am not going to be a part of playing gimmicks where we ask corporations to overpay their taxes so we can get around the 1974 Budget Act and pay-go and essentially be dishonest with the American people about what we are doing.

I understand I am not the chairman of the Finance Committee, but I am a member. And I am a Member of this body. Since I had no right in committee to offer an offset because they were ruled—they were going to be ruled nongermane, which they weren't, and now, consequently, we want to ram this through on a timed basis, I am not going to agree to that happening.

So we need to start acting like grownups in terms of our debt and not kick the can down the road 10 years, and that is what we are doing. We are going to use 10 years to pay for something we are going to spend over 3, just like we did on the highway bill, just like we violated pay-go, just like we violated the budget agreement we just agreed to last August. Now we are going to continue to do the same thing.

I have the greatest respect for my chairman. He has been here a long time. He knows a lot about these issues. I agree they need to happen, but they do not need to happen on the backs of taxpayers 10 years from now. We need to pay for what we are doing now.

That is the whole point of this exercise. I want us to be able to have certainty. I want us to have the Burma sanctions continued. I want us to do the right thing. But I want us to do it in the right way, and we are not. So that is where I stand.

I would defer to the chairman for his comments.

The PRESIDING OFFICER. The Senator from Montana.

Mr. BAUCUS. Mr. President, I very much understand the frustration of the Senator from Oklahoma, and I understand his reasons for objecting. In a perfect world, I might be sympathetic with his reasons, but this is not the perfect world. This is a world where we try to do our best to do our work and get legislation passed.

I personally don't have a problem with the Senator's suggestion that we could set 30 minutes aside and vote on his amendment as an alternate way to pay. I think the Senator understands this bill is fully paid for already. It is just the Senator would like it paid for in a different way.

The problem I have in trying to arrange all this and put it together is I can't control other Senators. Other Senators may object to the Senator's provision. They may have their own bills. In fact, I can think of two or three right now who would very much take advantage of a process where the Senator from Oklahoma strips out the bill and offers his own pay-for because they would say: Oh gosh, this is now an opportunity for me to offer mine. That is what they will say to themselves, and then we are really stuck because the Burma provisions expire, as the Senator knows, today. We can't dally. We can't wait. The AGOA provision expires at the end of September.

Now, one could say: Well, wait until the end of September. Unfortunately, a lot of American companies are uncertain whether we are going to extend past the September 30 date, and they are laying off people. Lots of job losses are already occurring as a consequence of the uncertainty. So my job, in putting together these several bills—including PNTR for Russia—in the committee was to talk to Senators and try to find an accommodation where we could get it passed.

I totally agree with the Senator on his main point; namely, how much fraud and waste there is and that it should be addressed and how important it is to get the debt down. As the Senator knows, yesterday, in committee, we talked about ways to address the so-called fiscal cliff, the very beginnings of the Finance Committee's finding solutions to the debt and some kind of grand bargain in the form of tax reform.

The Senator is correct. He did file amendments with alternative offsets, and I did state the amendments would be ruled nongermane. That is true. In my judgment, they were not germane. And he did suggest at that time that he wanted to offer an amendment on the Senate floor. As I said, I am not personally opposed to having a vote on the Senator's amendment as long as there is a limited time of debate. But I do think and believe others will object, and they will want to have their provisions passed. I just believe at this point it makes sense to proceed with AGOA, the DR-CAFTA bill, and the Burma bill, and deal with how we do offsets at a future date, not right now because it just gums up too much else.

The PRESIDING OFFICER. The Senator from Oklahoma.

Mr. COBURN. Mr. President, what the chairman said is this bill is paid for. I would put forward to the American public that if they went to Wendy's this afternoon and said: Give me a double cheeseburger; and, oh, by the way, over the next 10 years I am going to pay for it, most Americans would not say it is paid for.

What we are doing with this bill is taking custom user fees in the years 2021, 2020, 2019, and all the way down to pay for this bill. That is the problem. We will never solve our other problems until we get out of the mindset of saying because of the rules, we can stretch out the payment and call it paid for.

This bill isn't paid for. It is going to be paid for by the people who import things 10 years from now, not now. That is the whole point. That is why we have a $1.3 trillion deficit this year. That is why we have at least 2 to 3 million people unemployed in this country—because of our debt. So the question is, Is there a point in time when we are going to stop paying for things in the future and pay for them now? That is my objection.

I am fully open to passing this bill if somebody will just pay for it this year. If we are not going to pay for it this year, then we are not going to pass a bill by unanimous consent.

I will tell you, nobody else operates this way. Nobody rationalizes that you can pay—and the other thing, this is just $200 million. To everybody outside of Washington that is one ton of money. Here it is peanuts. To say we can't pay for something worth $200 million in a bill to do this, right now, to start the self-discipline of paying for it, it just says we are not worthy of being here if we would not do that.

So I would love to work out a solution, but there is a time and place where we have to change the direction of how we operate. For me, this is the bill that now says to me we are going to start paying for things. And if we can't pay for a $200 million pay-for in the same year, or at least the same 3 years we are going to actually spend it, then we are just not going to pass bills with my help.

I am not speaking for just TOM COBURN. The vast majority of Americans want us to pay for things by cutting wasteful spending. The fact that we are going to take custom user fees over 10 years to pay for this is ludicrous. Nobody in the rest of the economy can go out and say: Oh, by the way, I want to consume it now, but I will pay for it 10 years from now—interest free. It doesn't work that way, and we ought not to be doing it.

The chairman has my utmost respect. He has a tough job, I know that, of trying to do that. I will continue to try to work on solutions for this problem, but I am not moving from a position that we are going to pay for the things in the year in which we count them.

I yield the floor and I suggest the absence of a quorum.

The PRESIDING OFFICER (Mr. BROWN of Ohio). The clerk will call the roll.

The legislative clerk proceeded to call the roll.

Mr. LIEBERMAN. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. LIEBERMAN. Mr. President, may I ask what the pending business is now?

The PRESIDING OFFICER. The motion to proceed on S. 3414.

Mr. LIEBERMAN. Mr. President, I rise to speak on the motion to proceed to S. 3414, which is the Cybersecurity Act of 2012.

This cloture motion has been filed that will ripen sometime tomorrow, but I think it is the hope of Members on both sides of the aisle that we can proceed to vote on the motion to proceed today. I am hopeful colleagues on both sides of the aisle will vote to proceed, because although there continues to be some disagreement about the content of this bill and different approaches taken, I don't think there is any Member of the Senate who doesn't appreciate the fact that our country is currently under cyber attack every day, our businesses are victims of cyber theft every day, with the consequential loss of billions of dollars' worth of investments and, I would say, tens of thousands of jobs going elsewhere.

So this bill is not a solution in search of a problem; it is an attempt to solve a problem. Although there may be differences still on different components of the bill, I hope everybody will join together in at least saying: Let's proceed to the debate, and let's see if we can reach a conclusion before we leave for the August break next week.

I will report in this regard that this morning there was a second meeting held of those who have been most active in supporting different legislation that deals with the cyber threat to America. Senator COLLINS and I, Senator FEINSTEIN, Senator ROCKEFELLER, Senator CARPER—who introduced the pending matter, the Cybersecurity Act of 2012—Senators HUTCHISON and CHAMBLISS were there today, Senator COATS—who introduced the so-called SECURE IT Act—and then a group of peacemakers-bridge builders, Senators KYL and WHITEHOUSE, Senator GRAHAM, Senator COONS, Senator BLUMENTHAL, and Senator COATS, again, who sits in two of the three groups, which makes him a superbridge builder.

It was a very good, substantive discussion, in which we were all fleshing out the details of the various proposals. We are seeing some areas where

I think we feel we have a real opportunity to agree and some areas where it may be more difficult, but we haven't given up. But overall, I would say this process has been very encouraging. Basically, all the leading parties in the Senate and all the Senators are around the same table talking, which is very constructive to have happen. I appreciate that. To me, it is more reason to vote to proceed.

I wish to begin by thanking the aforementioned Senators COLLINS, ROCKEFELLER, FEINSTEIN, and CARPER, who joined me in sponsoring S. 3414, which I wish to talk about a bit now in this opening statement.

I also wish to thank the majority leader, Senator REID, for seeing the cyber threat to America in all its urgency and reality last year, urging Senator COLLINS and me to go forward and work on legislation, to work across party lines to get a bill out and now to thank Senator REID for keeping his commitment to bring this bill to the floor, even though, as always, there are clearly other important issues vying for this body's attention. But, to me, there is none more important to America's security and prosperity than this topic, which is cybersecurity and the cybersecurity bill that is now pending.

I would like to make three points in my remarks to my colleagues.

First is that the danger of cyber attacks against the United States is clear, present, and growing, with enemies ranging from rival nations to cyber terrorists, to organized crime gangs, to rogue hackers sitting at computers almost anywhere around the world. The pending matter, S. 3414, Cybersecurity Act of 2012, responds directly and effectively to this danger.

Second, this bill has been a long time in coming. In this regard, I note a letter sent out by the U.S. Chamber of Commerce overnight that, I must say, I found very disappointing overall because, if I may state it affirmatively, it doesn't embrace the same spirit I see Members of the Senate embracing; that although we have different positions, we can't afford to be inflexible. We can't be closed to compromise because of the urgency of the threat to our country and because of the general principle that has not been as evident in the Senate and Congress generally as it should be in recent years; that we never get anything done unless there is some compromise. I am not talking about compromise of principle. But if we go into every negotiation saying, I will only accept 100 percent of what I want, ultimately we are not going to get anything, if we can get 80 percent, 75 percent, 60 percent—particularly when we are dealing with a threat to the security of the United States and our prosperity as real as the cyber threat.

I hope our friends at the Chamber will reconsider the tone of their opposition and come to the table to talk with us about their concerns and see if we can't reach common ground because there is a larger national interest at stake than represented by any particular group or any individual Senator or their point of view.

In their letter of July 25, 2012, signed by R. Bruce Josten, executive VP for government affairs of the U.S. Chamber of Commerce, the Chamber says that:

> . . . S. 3414, the ''Cybersecurity Act of 2012,'' which has been rushed to the floor without a legislative hearing or markup. The bill was introduced just last week and remains a moving target; new and modified provisions of the bill are expected to be released in the coming days.

If they are, it is going to be a result of the give-and-take compromise that leads to legislation that is going on now. But I wish to respond to the idea that this came out of nowhere.

This bill has been a long time in coming. As a matter of fact, I went back and looked at the records. I attended my first hearing on cybersecurity as a member of the former Senate Governmental Affairs Committee—the predecessor to the current Homeland Security Governmental Affairs Committee—under the leadership of then-Chairman Fred Thompson. That was back in 1998, 14 years ago. I have been concerned ever since about the growing threat of cyber attack.

Along with my dear friend and colleague on the committee, Senator COLLINS, our committee has held multiple hearings on cybersecurity; that is, the new Homeland Security and Governmental Affairs Committee, and we weren't alone. There have been numerous hearings over the past several years and markups by multiple committees in both the Senate—many held by our colleagues Senator ROCKEFELLER and Senator FEINSTEIN in the Commerce and Senate Intel Committees—as well as in the House. Those deliberations and discussions were informed by numerous government and private sector studies on the dangers that lurk in cyberspace.

So this bill didn't come out of nowhere. We reported a bill out of our committee, with a lot of hearings and an open markup. We began, at the majority leader's direction, to negotiate with the other committees, particularly Commerce and Intel. We reached agreement, which is essentially what this bill is.

Incidentally, we then altered this bill—Senators COLLINS, FEINSTEIN, ROCKEFELLER, and I, in response to the bipartisan Kyl-Whitehouse group recommendations—to make it nonmandatory but still significant. So this bill has been aired and worked on and is ready for action.

But more to the point, the Senate needs to act. That is why it is so important we adopt the motion to proceed, because this threat is real, dangerous, and growing every day.

Third, this bill, S. 3414, is the result of bipartisan compromise. It is both bipartisan and it is the result of compromise. We cosponsors, as I mentioned, gave up some elements we thought were important that we had in our original bill. Given the cyber threat, we actually thought it was more important to move forward with a bill that will significantly strengthen our cybersecurity, even though it doesn't do everything we want it to do and thought should be done.

We didn't want to lose the chance to pass cyber legislation this year that could prevent a cyber 9/11 attack against the United States before it happens, instead of rushing in the midst of mayhem back to the Senate and House to adopt cybersecurity legislation after we suffer a major attack.

As I said, we have incorporated ideas from Senators WHITEHOUSE, KYL, and the other Members whom we were working with quite diligently to help us find common ground. I wish to explicitly and enthusiastically thank them for their efforts.

We have heard and responded to Senators DURBIN, FRANKEN, WYDEN, and others, and advocacy groups across the political spectrum from left to right, who have pressed for greater protections for privacy, personal privacy in this bill. We have made substantial changes designed to address concerns from stakeholders and colleagues.

I am confident we can work through more issues as we debate the bill on the floor. But the main point here, if I may use quite a familiar expression around here with a slightly unique follow-on phrase, I hope: If in our quest for cybersecurity legislation we allow the perfect to be the enemy of the good, we are going to end up allowing our enemies to destroy a lot that is good in the United States of America. We have to act together for the good of the Nation, get the debate started and bring amendments to the floor for an up-or-down vote.

Let me stress at this point that Senator REID, the majority leader, has been quite clear that his desire, his intention is to have the process be an open amendment process so long as the amendments are germane and relevant to the topic of the bill, cybersecurity, not just open to any amendment about any subject.

I want to go back over these three points and talk about them in a bit more detail. Let me start with the reality of the threat. I want to read from a letter sent to us recently by some of our Nation's most experienced security leaders from both Republican and Democratic administrations. Here is a letter to the majority and minority leader, signed by former Bush administration Secretary of Homeland Security Michael Chertoff; former Bush administration Director of National Intelligence ADM Mike McConnell; former Bush Deputy Defense Secretary Paul Wolfowitz; former NSA and CIA Director General Michael Hayden; former vice chair of the Joint Chiefs of Staff Marine Gen. Jim Cartwright; and former Deputy Defense Secretary William Lynn. I quote from the letter. It

is quite an impressive group, clearly bipartisan—nonpartisan.

We write to urge you to bring cybersecurity legislation to the floor as soon as possible. Given the time left in this legislative session and the upcoming election this fall, we are concerned that the window of opportunity to pass legislation that is in our view critically necessary to protect our national and economic security is quickly disappearing.

These security leaders went on to say:

Infrastructure that controls our electricity, water and sewer, nuclear plants, communications backbone, energy pipelines and financial networks must be required to meet appropriate cybersecurity standards. We carry the burden of knowing—

It is really chilling.

We carry the burden of knowing that 9/11 might have been averted with the intelligence that existed at the time. We do not want to be in the same position again when ''cyber 9/11'' hits—it is not a question of whether it will happen—but when.

That is not a statement from a Member of the Senate or an advocate on one side or the other. These are proven national security leaders who have worked in administrations of both political parties. ''It is not a question of whether a cyberattack will happen,'' they say, ''but when.''

Many others have issued similar warnings. Secretary of Defense Panetta has said the next Pearl Harbor-like attack against America will be launched from cyberspace.

Chairman of the Joint Chiefs of Staff Gen. Martin Dempsey has warned: ''A cyberattack could stop our society in its tracks.''

Just this month, National Security Agency Cybercommand Chief Gen. Keith Alexander blamed cyber attacks for: ''The greatest transfer of wealth in history.''

General Alexander estimated that American companies lose about $250 billion a year through intellectual property theft through cyberspace; $114 billion to theft through cyber crime; and another $224 billion in downtime the thefts caused.

We talk a lot here in the Senate these days, as we must, about how we protect American jobs. It turns out that in creating more cybersecurity in our country we are also going to protect tens of thousands of jobs which otherwise are going to end up elsewhere in the world because they will have stolen the industrial secrets that lead to the new industries that create those jobs.

General Alexander concluded this part of the statement he made by saying: '' . . . this is our future disappearing before us.''

Cyber attack.

These fears are not speculative. Let me go through a recent op-ed in the Wall Street Journal that President Obama wrote.

In a future conflict, an adversary unable to match our military supremacy on the battlefield might seek to exploit our computer vulnerabilities here at home. Taking down vital banking systems could trigger a financial crisis. The lack of clean water or functioning hospitals could spark a public health emergency. And as we have seen in past blackouts—

Which were caused by natural disasters, for instance—

the loss of electricity can bring businesses, cities and entire regions to a standstill.

These fears are not speculative. They are not theoretical. They are based on existing facts and existing vulnerabilities. Consider, if you will, this recent story in the Washington Post that detailed how a young man living an ocean away used his computer to hack into the control panel of a small town water utility in Texas. It took him just 10 minutes and required no special tools or training. The utility had no idea of what had happened until the hacker posted screen shots of his exploit online as a warning of how vulnerable all of us are. Imagine if terrorists decided to target a string of small utilities across the United States and either cut off fresh water or dumped raw sewage into our lakes, rivers, and streams. We would have an environmental and economic disaster on our hands. But this is a real possibility.

This brings me to my second point. We need to act and act now. The challenge of cybersecurity has been studied for a long time and there is no need for more studies or hearings or delay, as the Chamber letter requests. I went back to the Congressional Research Service. According to a report that they issued, in the 112th Congress alone there have been 38 hearings and 4 markups in the House and 33 hearings in the Senate on cybersecurity.

In the 112th Congress, the Judiciary Committee also held a markup on the Personal Data and Privacy Security Act and in previous Congresses the Senate has held markups on cybersecurity legislation in five separate committees under regular order, all of which is included in the bill that is pending before us today.

Since 2005, the Senate Homeland Security Committee alone has held 10 hearings with 48 witnesses testifying and took questions over a total of 18 hours. Look at the bill's cosponsors. S. 3414: Senators COLLINS and I, along with Senators FEINSTEIN and ROCKEFELLER, have held numerous hearings, forums, and cybersecurity demonstrations for Members and staff. All these hearings and briefings were further informed by, according to the CRS, a total of 60 governmental reports totaling 2,624 pages produced by the GAO, the Department of Defense, the OMB, the Department of Energy, and other Federal agencies. This doesn't count the many more reports from the private sector—computer security firms such as SEMANTEC and think tanks and academic institutions such as MIT and the Center for Strategic and International Studies.

This matter is ready for action. I go back to a 1936 book Winston Churchill wrote, ''When England Slept.'' Not ''Why England Slept'' but ''When England Slept'' . He asked his colleagues in the Parliament who were refusing at that time to act decisively to counter the rise of German military power despite its clear threat to Europe—Churchill said: ''What will you know in a few weeks about this matter that you do not know now . . . and have been not been told any time in the last six months?''

I think the same can be said now. That is why I think it is so important to adopt the motion to proceed and get something done before we leave Washington for the August break.

Finally, in the interest of moving forward, my cosponsors and I, as I indicated earlier, have made a major compromise in the bill we are bringing to the floor in terms of how we deal with critical cyber infrastructure. Here again, we are talking not about small businesses around America, we are talking about powerplants, energy pipelines, water systems, financial systems that we all depend on for our banking, water—sewer systems, for instance—that if sabotaged or commandeered in a cyber attack could lead to catastrophic deaths and economic and environmental losses.

In our original bill, Senators COLLINS, FEINSTEIN, ROCKEFELLER, and I called for mandatory cyber safety standards for all critical infrastructure after those standards were developed in consultation with the private sector. We did not think this was a unique or onerous requirement but our responsibility in carrying out our constitutional oath to provide for the common defense. Since antiquity, as a matter of fact long before the American Constitution, societies have chosen to adopt safety standards to protect their citizens, particularly safety standards for physical structures starting with the homes we live in, but also our offices, factories, and critical infrastructure such as powerplants and dams. Today we call these building codes. Can you imagine if there were no building codes, the danger that people would take when they walked in our office buildings or factories or apartment houses or residences?

I cannot resist saying these building codes in some sense are as old as the Bible. Here I go to Deuteronomy 22:8 which says:

When you build a new house, you shall build a parapet for your roof, so you shall not bring the guilt of blood upon your house if anyone should fall from it.

There is direct relevance in a very different context from the Biblical context to what we are trying to do here, which is to build a kind of parapet around our cyber systems so we do not bring the guilt of blood on us because somebody has attacked through those cyber systems.

The reason we have done this over antiquity in the physical world is obvious. If one of our homes catches fire because of the wiring not up to code or it happens in an apartment building or an

office building, the people in it are endangered, obviously, but also the lives and homes of our neighbors, the community are in danger as well. Numerous bipartisan national security experts have been in total agreement that mandatory requirements are needed to protect our national and economic security from the ever-rising risk of cyber attacks.

But it was this provision, seen in the context of regulation of business while we were seeing it as homeland security, protecting homeland security, that was the most controversial in our compromise bill and drew the most criticism. To be more specific about it, it threatened to prevent passage of any cybersecurity legislation this year which, for the sponsors of this bill, was simply an unacceptable result.

Following the rule that no matter how deeply one believes in the rightness of a provision in a bill, we agreed to change it because there is so much else that is critically important in our bill that will protect America's cybersecurity. So we withdrew the mandatory provision and created all the standards for performance of how the most critical infrastructure, cyber structure, would protect itself. But then we left it voluntary; however, we did create some incentives. Let me be clear that the decision is to be what we all want it to be, which is as a result of a collaborative, cooperative effort that businesses that operate the most critical cyber structure, such as, electrical systems, water systems, transportation, finance, communications, will want to comply.

Under our revised bill, private industry, which incidentally owns as much as 85 percent of the Nation's critical infrastructure—that is the American way, and that is great. But when that 80 to 85 percent of our critical infrastructure can well and probably will be the target of not just theft but attacks by enemies of the United States, we have to work together to prevent that.

In our bill we give the private sector the opportunity to develop a set of cybersecurity practices which will then be reviewed by the new National Cybersecurity Council that our bill creates. It will be chaired by the Secretary of Homeland Security and made up of representatives of the Department of Defense, Commerce, Justice, and the intelligence community, and presumably the Director of National Intelligence. This National Cybersecurity Council will review the standards agreed upon by the private sector and decide whether they are adequate to provide the necessary level of cybersecurity for the American people.

Owners of critical infrastructure will then have a decision to make. Do they want to essentially opt into the system or do they want to not do so? That is up to them under the bill as is put before them because it is voluntary. If they opt in—and this is what we hope will be an incentive—they will be entitled to receive some benefits, the most significant of which will be immunity from certain forms of liability in case of a cyber attack. We also offer expedited security clearances and prioritize technical assistance from our government on cyber questions from those critical covered cyber-infrastructure companies that opt into the system.

I think our colleague from Rhode Island, Senator WHITEHOUSE, has a very good metaphor for what we are trying to do. As he said, we are trying to build Fort Cybersecurity where we essentially become part of a system that provides greatly enhanced protection from cyber attack and cyber theft, but we are not compelling anybody to come into Fort Cybersecurity. We are encouraging them to do so, and we are giving them some incentives to do so. Of course, we hope that sound and wise administrators of those companies and forces of the marketplace will encourage them to make a decision to come into Fort Cybersecurity.

Finally, our bill contains information-sharing provisions, which I think most people who have looked at the threat of cyber attack and cyber theft think are very important. These provisions will allow the private sector and government to share threat information between each other and among themselves. In other words, one private company can share information about an attack with another private company to see if the attack is part of a broader pattern.

For instance, they can talk about where it may be coming from to raise their cyber defenses against it, and to do so without fear of—well, for instance, any trust action by the State or Federal Government. Also, very often companies that believe they have been a victim of cyber attack will go to the Federal Government, the Department of Homeland Security, or the National Security Administration for help; however, a lot of them don't. Part of the reason for that is they fear, among other things, they may compromise the privacy of their records. Others, quite frankly, don't want to admit they have been attacked. This is a real problem. I will come back to that in just a moment.

We give protection from liability for companies that share their information with the government. Yet there were many individual Senators and many people from outside groups who are focused on privacy who were concerned that in doing this we were opening up a method by which parts of our Federal Government could basically violate privacy restrictions, take personal information off of the information shared by a private company with the government, and they be the victim of some kind of public intrusion or even law enforcement.

So I think we negotiated a good series of agreements on this which, one, will ensure that companies who share cybersecurity information with the government give it directly to civilian agencies and not to military agencies. That was a concern people had.

Second, we ensure that information shared under the program be reasonably necessary and described as a cybersecurity threat. In other words, not just wantonly share it because some of this is private information.

Third, we restrict the government's use of information it receives under the cyber information-sharing authority so that it can be used only for actual cybersecurity purposes and to prosecute cyber crimes with two exceptions broadly agreed on: One is that the information can be used to protect people from imminent threat of death or physical harm; and, two, to protect children from serious threats of one sort or another.

Next, we would require annual reports from the Justice Department, Homeland Security, the defense and intelligence community, and inspectors general to describe what information has been received in the previous year, such as, who got it and what was done with it. Finally, we allow individuals to sue our government if the government intentionally or willfully violates the law; that is to say, the law relating to these privacy protections.

I am very pleased by these changes we made. I want to say this loudly and clearly: This bill is about cybersecurity. But in trying to elevate our cybersecurity, we didn't want to compromise people's privacy or their freedom. So what I have just read was intended to assure that this bill, as best we could, would not compromise privacy or freedom rights.

Then I took this set of compromises to the most important people in our government who are focused on cybersecurity—the Department of Homeland Security, the National Security Agency, the FBI—and they all said, I am pleased to say, these privacy protections will not inhibit their ability to protect America's cybersecurity. They can live with these without the slightest diminishing of their focus, which understandably is not privacy but it is cybersecurity. They said these amendments to our original bill don't inhibit what they are doing.

I conclude by, again, urging my colleagues to vote, presumably today, yes on the motion to proceed so we can get the debate started, so we can continue to work to achieve common ground and a meeting of the minds and enact this piece of crucial national and economic and security legislation in this session of Congress.

I thank the Chair, and I yield the floor.

The PRESIDING OFFICER. The senior Senator from Texas.

Mrs. HUTCHISON. Mr. President, I have listened to the distinguished Senator and chairman of the Homeland Security Committee and the presentation of the bill that I assume will be voted on today. I appreciate very much that we have had the meetings. There are really two bills that have been introduced: the Lieberman-Collins, bill with their cosponsors, and then I have introduced legislation called the SECURE

IT Act along with Senators MCCAIN, CHAMBLISS, GRASSLEY, MURKOWSKI, COATS, JOHNSON, and BURR. These are eight ranking members of committees and subcommittees who have jurisdiction over cybersecurity, and we differ in a major way from the bill that is before us that is cosponsored by the Chair and ranking member of the Homeland Security Committee. All the other ranking members of the committees that have jurisdiction, are in disagreement with their approach.

Now, the good news is we have been meeting to try to begin to work out the differences and see if we can move forward. Our bill, the SECURE IT bill, will be introduced as an amendment in the nature of a substitute if, in fact, we take up the bill today.

I would agree with what Senator LIEBERMAN said right off the bat in that I believe, as long as we have an open amendment process, we will vote to move to the bill. I don't think anyone in our group or anyone with whom I have talked wants to hold up dealing with cybersecurity. We know America's systems could be under threat, and some have been hacked into already. There are terrorists who seek to sabotage networks. There are people who want access to proprietary information and intellectual property. We need to protect our systems and our country against those attacks, which is why as long as we have an amendment process and we are not shut out from discussing this, we will vote to move forward to the bill.

This bill was not marked up in committee. It did have a lot of hearings in committee. Since it wasn't marked up, amendments were not able to be introduced and discussed and voted on, which makes it harder, as we all know, when we come to the floor with a bill where there are major disagreements. We have not had the capability for the committee to take up the amendments and vote on them. That is why I think we need to have the open amendment process and why we do want to move forward on the good faith that it will be open.

Now, our bill, the SECURE IT Act, is centered on consensus items. It sets aside the controversial provisions that are of questionable need, and it is also one that we believe we can work with the House on to pass and send to the President. The bill we have would greatly improve information sharing to and from and with the government with other private sector industries in the same field, and we think that is the most important step we could all take on a fairly quick basis to start the process of getting more security throughout our systems.

We must also ensure that the entities and government and industry share information back and forth. It has to be a two-way street. Obviously, if an industry is going to share information about potential threats, if they see risks or they see problems in a system, it must get information from the government agencies that are doing the intelligence gathering on a quick basis.

Our bill also dramatically improves cybersecurity for Federal agencies themselves. It does update the rules that govern cybersecurity, and it requires any government contractor to inform their agency clients if their clients' systems are under a significant risk or attack. We think that is reasonable as a part of a government contracting requirement.

Today antitrust laws and liability concerns inhibit private companies from exchanging the information that is necessary to defend against and respond to cyber threats. If a company is going to be encouraged to share information with a competitor about cyber threats, they have to know they are not going to be then hit with an antitrust lawsuit. I think that is pretty clear. So our bill does address that. We make it very clear there are antitrust immunities as well as most certainly immunity from a lawsuit if they provide information on a voluntary basis. If they are sued, and they have acted in accordance with our bill, then they would have protection from liability for a lawsuit on cyber attack. So those are the things we do that I think will open up the information sharing, which is the way we believe it is important as the next step.

It is also very important that we have the safeguards for privacy. I do believe the underlying bill certainly protects privacy, and so does our substitute. We have safeguards that protect the privacy and civil liberties of all Americans while we preserve the right to ensure that we try to protect America in general from attack from the outside.

We also in our bill improve the security of Federal information systems and facilitate the prosecution of cyber crime. We want to beef up protections against criminals who are hacking in, as well as potential terrorists who might, in order to be able to prosecute against cyber crime as a disincentive to break the law.

Finally, our legislation has broad industry support. The businesses in the private sector that know their systems best and that fight every day to protect their systems and networks believe SECURE IT is the best way to go. We believe that with the cooperation of the business community, without having a big regulatory morass, is the way we are going to get the most cooperation from the people who are running the networks and systems.

I have letters of endorsement from the U.S. Chamber of Commerce, the National Association of Manufacturers, the American Fuel and Petrochemical Manufacturers, the American Petroleum Institute, U.S. Telecom, National Retail Federation, the Internet Security Alliance, and I ask unanimous consent that these letters be printed in the RECORD.

There being no objection, the material was ordered to be printed in the RECORD, as follows:

CHAMBER OF COMMERCE OF THE
UNITED STATES OF AMERICA,
Washington, DC, June 29, 2012.

Hon. JOHN MCCAIN,
U.S. Senate,
Washington, DC.
Hon. KAY BAILEY HUTCHISON,
U.S. Senate,
Washington, DC.

DEAR SENATORS MCCAIN AND HUTCHISON: The U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than three million businesses and organizations of every size, sector, and region, supports S. 3342, the ''SECURE IT Act of 2012.'' This bill would dramatically help the United States improve its cybersecurity posture and serve as a catalyst for greater sharing of targeted cyber threat information between the government and the private sector.

The Chamber agrees that the right path forward is for the public and private sectors to work together in solving mutual challenges, increasing real-time cyber threat information sharing between and among the public and private sectors, and fostering the development and deployment of innovative cybersecurity technologies. This path provides the best opportunity of staying ahead of fast-paced cyber threats.

The Chamber also agrees that Congress should not layer additional cybersecurity regulations on the business community. New compliance mandates would automatically drive up costs and misallocate business resources in a tough economy without necessarily increasing security. Critical infrastructure owners and operators already devote significant resources toward protecting and making their information systems more resilient because it is in their overwhelming interest to do so and good for the country.

Another positive aspect of S. 3342 is that it would leverage existing information-sharing and analysis organizations and incorporate lessons learned from pilot programs undertaken by critical infrastructure sectors. Both offer complementary, demonstrated models to enable the government to share cyber threat information with the private sector in a trusted, constructive, and actionable manner without creating burdensome regulatory mandates or new bureaucracies.

S. 3342 would also provide businesses the much-needed certainty that threat and vulnerability information shared with the government would be provided safe harbor and not lead to frivolous lawsuits, would be exempt from public disclosure, and would not be used by officials to regulate other activities. The Chamber welcomes your efforts to make certain that the information-sharing processes in your bill include necessary privacy and civil liberties protections, such as tightening the definition of cyber threat information.

The Chamber appreciates your efforts to address an array of industry concerns. As the SECURE IT Act progresses, we look forward to working with you to tailor the scope of information that certain entities in the private sector could be required to provide a government agency or department under statute.

Equally, we want to ensure that government entities continue to acquire the most innovative and secure technology products and services under provisions of S. 3342 related to reforming the Federal Information Security Management Act. Federal officials who manage agencies' information security programs should leverage industry-led, globally accepted standards for security assurance during the acquisition process. Added language stipulating that the bill would not convey any new regulatory authority to agencies or departments is a step in the right direction.

The Chamber believes that your bill highlights the notion that Congress should focus on enacting legislation that would truly improve the sharing of actionable and targeted information between public and private entities in order to defeat our mutual adversaries—not layering additional regulations on the business community. We appreciate your commitment to a nonregulatory approach to bolstering collective security; it is one that the Chamber strongly supports.

Sincerely,

R. BRUCE JOSTEN.

NATIONAL ASSOCIATION OF MANUFACTURERS,
Washington, DC, March 26, 2012.

Hon. JOHN MCCAIN,
U.S. Senate,
Washington, DC.
Hon. KAY BAILEY HUTCHISON,
U.S. Senate,
Washington DC.

DEAR SENATOR MCCAIN AND SENATOR HUTCHISON: On behalf of the 12,000 members of the National Association of Manufacturers (NAM), the largest manufacturing association in the United States representing manufacturers in every industrial sector and in all 50 states, I am writing to express the NAM's support for S. 2151, the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act or ''SECURE IT'' Act.

Manufacturers through their comprehensive and connected relationships with customers, vendors, suppliers, and governments are entrusted with vast amounts of data. They hold the responsibility of securing this data, the networks on which it runs, and the facilities and machinery they control at the highest priority level. Manufacturers know the economic security of the United States is directly related to our cybersecurity.

The NAM supports the government sharing timely and actionable threat and vulnerability information with the private sector. We also support the creation of a voluntary framework that allows companies to share information with the government and with each other without creating new liabilities.

NAM member companies also support allowing the private sector to continue developing appropriate general and industry-specific best practices in collaboration with the Federal government for improved security. Encouraging manufacturers to adopt industry-standard best practices through incentives is the best way to ensure innovation while addressing the evolving threats to our nation's security. In contrast, mandates on the use of specific technologies or standards and imposing a prescriptive regulatory framework would unduly inhibit innovation.

The SECURE IT Act addresses these issues important to manufacturers. The bill would allow for voluntary information sharing across the cyber community and protect information owners from liability stemming from those actions. It would also help secure government networks, increase the penalties for cybercrime, and prioritize cybersecurity research using existing government dollars. The SECURE IT Act does this without creating a new and unnecessary regulatory burden on manufacturers.

The NAM and all manufacturers remain intensely committed to working with Congress to secure our cyberinfrastructure from harm. We look forward to thoughtful discussions and examination by all the Committees with jurisdiction on this issue to ensure that any legislation that moves forward mitigates the cyber threat facing our nation.

Sincerely,

BRIAN J. RAYMOND,
Director, Technology Policy.

AMERICAN FUEL & PETROCHEMICAL MANUFACTURERS,
Washington, DC, March 13, 2012.

Re AFPM supports the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology (SECURE IT) Act.

Hon. HARRY REID,
Senate Majority Leader,
U.S. Senate, Washington, DC.
Hon. MITCH MCCONNELL,
Senate Republican Leader,
U.S. Senate, Washington, DC.

DEAR SENATORS REID AND MCCONNELL: AFPM, the American Fuel and Petrochemical Manufacturers (formerly National Petrochemical & Refiners Association), writes today to express its support for S. 2151, the ''Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology (SECURE IT) Act of 2012 '' introduced by Senators McCain, Hutchison, Grassley, Chambliss, Murkowski, and Coats. This important legislation breaks down current barriers to information sharing to ensure greater security without interfering in the ability of private-sector businesses to protect their own IT systems.

AFPM is a trade association representing high-tech American manufacturers of virtually the entire U.S. supply of gasoline, diesel, jet fuel, other fuels and home heating oil, as well as the petrochemicals used as building blocks for thousands of products vital to everyday life. Protection of our members' Information Technology (IT) and Industrial Control Systems (ICS) are critical to the fuel and petrochemical manufacturing process.

The SECURE IT Act opens avenues to foster greater information sharing between the private sector, non-federal government agencies, and Federal cybersecurity centers, allowing private companies to voluntarily share information without concern of antitrust and liability violations. Instead of creating a massive regulatory regime under the Department of Homeland Security, this legislation recognizes the proactive role the refining and petrochemical industries have taken to protect our facilities. The sharing of information among companies, as well as with the federal government, will improve our preparedness for an attack and better educate our companies' employees on the various threats facing all critical infrastructures.

AFPM's members remain concerned over alternative approaches to cybersecurity that would create an environment focused simply of compliance with bureaucratic government regulation, rather than on actual security. Because cyber threats and crimes are always changing, establishing a one size fits all regulatory framework for our facilities could create more vulnerabilities and has the potential to make existing cybersecurity protections significantly less effective.

Cybersecurity is critical to protecting refineries and petrochemical facilities. Breaking down the barriers to information sharing will ensure our security and provide our facilities with timely information to better protect our systems against attack. AFPM believes that the SECURE IT Act will make America and its IT and ICS systems more secure and urges your support for this legislation.

Sincerely,

CHARLES T. DREVNA,
President, AFPM.

API,
Washington, DC, March 7, 2012.

Hon. HARRY REID,
Senate Majority Leader, U.S. Senate,
Washington, DC.
Hon. MITCH MCCONNELL,
Senate Republican Leader,
U.S. Senate, Washington, DC.

DEAR SENATORS REID AND MCCONNELL: We are writing to express our support for S. 2151 ''SECURE IT Act of 2012'', which was recently introduced by Senators McCain, Hutchison, Chambliss, Grassley, Murkowski, Coats, Burr and Ron Johnson. The American Petroleum Institute is the national trade organization representing nearly 500 companies involved in all aspects of the domestic oil and natural gas industry.

We appreciate the balanced and carefully crafted approach taken in S 2151, using and improving upon sector-based cybersecurity processes and partnerships already in progress, and working toward increased collaboration between government and industry rather than imposing additional and unworkable regulations. For example, the sharing of timely and actionable information on cyber threats, vulnerabilities and mitigation procedures will help companies improve their detection, prevention, mitigation and response capabilities. Continuing to improve valuable information sharing, both between a company and the government and among companies within industry sectors, is an effective tool in advancing our nation's cybersecurity.

We remain concerned that alternative legislative approaches under consideration could have unintended consequences on business and industry, including the diversion of resources away from activities that will reduce or mitigate risks associated with daily cyber threats in order to comply with mandates that would soon be outdated.

Cyber threats change rapidly. API believes the proposed path to improved information sharing will encourage the public and private sectors to work together to reduce risk and promote investment in new technologies to keep industry cyber systems secure. Legislation must enhance, rather than impede, innovative processes and encourage advancements in new cyber risk assessment and mitigation measures.

API recognizes the leadership of the ''SECURE IT Act'' sponsors in addressing our nation's cyber security challenges. We appreciate the continued commitment to offer valuable solutions on this complex issue and look forward to working together in the days and weeks ahead.

Sincerely,

MARTY DURBIN,
Executive Vice President.

NATIONAL RETAIL FEDERATION,
Washington, DC, June 27, 2012.

Hon. JOHN S. MCCAIN,
U.S. Senate, Russell Senate Office Building, Washington, DC.

DEAR SENATOR MCCAIN: The National Retail Federation strongly supports your efforts to craft effective cybersecurity legislation to protect our nation's critical infrastructure from cyber-attacks and we appreciate and applaud your introduction today, June 27, of S. 3342, the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012 (the ''SECURE IT Act''). In your efforts to develop a bipartisan bill for Senate floor consideration, we urge you and your cosponsors to ensure that all provisions of the bill support the overall purpose of protecting our critical infrastructure and are not expanded to include unrelated or unvetted amendments, such as data breach and commercial privacy legislation.

As the world's largest retail trade association and the voice of retail worldwide, NRF represents retailers of all types and sizes, including chain restaurants and industry partners, from the United States and more than 45 countries abroad. Retailers operate more than 3.6 million U.S. establishments that support one in four U.S. jobs—42 million working Americans. Contributing $2.5 trillion to annual GDP, retail is a daily barometer for the nation's economy. NRF's Retail Means Jobs campaign emphasizes the economic importance of retail and encourages policymakers to support a Jobs, Innovation and Consumer Value Agenda aimed at boosting economic growth and job creation.

The SECURE IT Act advances the important goal of facilitating cooperative information sharing about cyber threats between the government and private sector, a key component of cybersecurity legislation we support. The goals underlying cybersecurity legislation and provisions in data breach notification legislation are fundamentally contradictory. The cybersecurity proposals encourage information sharing by limiting companies' liability for that sharing. On the other hand, some proposed breach notification bills either penalize companies for sharing news of a breach, by imposing onerous credit monitoring obligations, or impose lesser civil penalties for failing to disclose a breach in the first instance. Juxtaposing these contrasting proposals would place businesses in a precarious position when their systems are attacked by cyber criminals. Thoughtful examination and comparison of the SECURE IT Act with proposed data breach legislation reveal that they are not properly aligned.

A similar case exists with respect to commercial privacy legislation called for by the Obama Administration in its Privacy and Innovation Blueprint and by the Federal Trade Commission in its final privacy report. Comprehensive consumer privacy legislation, which has not been vetted by any committees of jurisdiction in the Senate, attached to the SECURE IT Act, flies in the face of the deliberative process that this sensitive topic deserves.

Congress must strike the careful balance between consumers' privacy interests and the provision of goods and services over the Internet that the average American consumer expects in this e-commerce economy. That type of careful deliberation, we fear, may not take place on the Senate floor at this time. Furthermore, these commercial privacy provisions are unrelated to the core purposes of cybersecurity legislation, and Congress has ample time to fully consider the positions and concerns of all stakeholders in a separate and unrushed legislative process.

NRF is supportive of your efforts to create a cybersecurity bill that is based on fully vetted concepts that will aid in protecting our nation's most critical infrastructure but that is not encumbered with conflicting amendments addressing data breach notification or insufficiently examined new privacy regimes. NRF looks forward to working with you on this legislation moving forward.

Sincerely,

DAVID FRENCH,

Senior Vice President, Government Relations.

Mrs. HUTCHISON. Mr. President, our bill also allows for a true collaborative effort.

The reason we are not supporting the bill that is on the floor today is because we believe it does not do the priorities that we can pass, and it does increase the mandates and the regulatory overkill, in our opinion, that will keep our companies from being able to move forward on an expedited basis to start protecting our systems.

A priority of mine throughout this process has been that we help the private sector combat cyber attacks by breaking down the barriers to sharing information. If we could take that one step, we would be a long way toward ensuring that we are increasing the security of all Americans. The bill before us will actually undermine current information sharing between the government and the private sector. That bill's information-sharing title is a step backward because it slows the transfer of critical information to our intelligence agencies, and there is not sufficient protection from antitrust. In addition, there is no consensus in the Senate to grant the Department of Homeland Security broad new authority to impose burdensome regulations on the private sector.

While I am pleased our colleagues who are cosponsoring the bill that is before us have made an effort to move away from direct regulation of our Nation's systems, it has a long way to go. While their bill allows the private sector to propose standards that are described as voluntary, the bill actually empowers Federal agencies to make these voluntary standards mandatory. If an agency does not make the standards mandatory, it would have to report to Congress why it had failed to do so. That is a pretty big incentive for mandates to start being put on with regulations that will be required.

I believe there is a way forward. If the Senate takes the well-reasoned and broadly supported provisions of the SECURE IT bill and puts them with a voluntary and industry-driven critical infrastructure protection title, we could pass a Senate bill with overwhelming support.

The key to reaching consensus has five parts:

The cybersecurity standards must be developed by the private sector and must be truly voluntary. The relationship between government and the private sector in this area must be cooperative, not adversarial and not regulatory.

The National Institute for Standards and Technology should be the convening authority for the private sector standard-setting process. The government can have a role in ensuring the standards are sufficient, and it should, but it can't establish a regulatory regime that will lengthen and hamper the efforts to open information sharing.

Companies—and here is the incentive for the companies to do exactly what we are asking them to do—companies that adopt the voluntary standards must receive robust and straightforward protections from liability as well as necessary antitrust and Freedom of Information Act exemptions. If a company is going to turn over its proprietary information to the government, it must be protected from freedom of information requests from the government that then would take its private proprietary information public.

As in the SECURE IT Act, the information-sharing title must be strong and encourage the private sector to share information, and it must encourage the government to share with the private sector. It cannot cut out those with the most expertise in the area, meaning the national security agencies should not have to be subservient to the Department of Homeland Security.

In addition, a 5-year sunset would allow Congress to revisit the act and make needed changes. FISA has certainly shown that with a sunset, it allows the flexibility to adapt to new issues that arise and stay current in its processes to deal with cybersecurity. We believe a 5-year sunset would be the right amount of time to get this going, set things in place, see what works, and see what needs to be adjusted.

I am hopeful my colleagues and I can come to a compromise on this critical issue. We want a strong cybersecurity bill. We want one that can pass both Houses. The five points I have laid out could get us to a bill that will significantly take the steps to improve our Nation's cybersecurity.

I wish to read a couple of excerpts from the Heritage Foundation's views of the bill that is before us today:

Cybersecurity legislation will likely be taken up by the Senate tomorrow.

This was written yesterday.

Regrettably, the idea that we just need to do something about cybersecurity seems to be trumping the view that we need to do it right.

The Cybersecurity Act of 2012, authored by Senators Lieberman and Collins, seeks to solve our cybersecurity ills but only threatens to make the situation worse.

The ''voluntary'' nature of the CSA's standards is also questionable. Any voluntary standard is one step away from mandatory, and Senator Lieberman has already indicated that if the standards aren't voluntarily used, he would push to make them mandatory.

Even more concerning, section 103(g) of the CSA gives current regulators the power to make these ''voluntary'' standards mandatory.

It specifically authorizes that action.

If a regulator doesn't mandate the standards, the regulatory agency will have to report to Congress why it didn't do so.

Again, there is strong encouragement to just make the standards mandatory and avoid a congressional inquisition.

Finally, the Heritage Foundation goes on to say:

Finally, the sharing and analysis of cybersecurity threat information was weakened by confining cybersecurity information exchanges to civilian organizations. Though in an ideal world the Department of Homeland Security would have the capability to lead our cybersecurity efforts, it currently lacks those capabilities and needs to lean on more capable organizations such as the National Security Agency. The recent changes, however, give DHS more responsibility than it is likely able to handle.

So we will certainly move forward with the understanding that we will

have the ability to offer amendments and try to make this a workable bill. It is certain that because the committee was not able to mark up the bill, we have to have the amendments to try to perfect it.

I would very much like to take the first step forward in cybersecurity, which is why, assuming we have the right to amend, I will support going to the legislation so that we can start the amendment process next week. I think the people who are cosponsors of my legislation, along with Senator MCCAIN, Senator CHAMBLISS, Senator GRASSLEY, Senator BURR, Senator MURKOWSKI, Senator COATS, and Senator JOHNSON, want to make sure we do this right. As the Heritage Foundation has so aptly said, we don't want a big, new regulatory scheme that is not going to be successful in our efforts to improve the cybersecurity safeguards in our system.

We are the ranking members of all but one of the relevant committees. We know this area. We deal with the agencies that deal with cybersecurity and all of the national security in our country. We know what can work, we know what we have a chance to pass, and we know how to take the first step forward without another big regulatory overreach, as we have seen happen in the last 3½ years in this administration. We hope to work with the majority, with the Lieberman-Collins bill, and come up with something that everyone will feel is the right step forward. We would like to have a bill that will get a large number of votes rather than a very lopsided vote against it.

I appreciate very much that we are now beginning to discuss this. I am appreciative that we have had several meetings with all of the sides that have been put forward as having concerns with the bill that is on the floor as well as its sponsors. I hope we can keep working toward a solution that will protect America and do it in the right way.

Thank you, Mr. President. I yield the floor.

The PRESIDING OFFICER. The senior Senator from Arizona.

Mr. MCCAIN. I thank the Chair. I ask unanimous consent to take 5 minutes in morning business and then speak on the pending legislation.

The PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

TRIBUTE TO AMBASSADOR RYAN CROCKER

Mr. MCCAIN. Mr. President, I would note that I saw my friend Senator LIEBERMAN on the floor a second ago, and I know he joins with me in this statement.

I wish to take a few minutes to pay tribute to Ambassador Ryan Crocker, who ended his tour this week as the U.S. Chief of Mission in Kabul, Afghanistan.

As some of my colleagues may know, Ambassador Crocker's health has unfortunately been poor, so he is returning to receive some much needed care. But what my colleagues may not know is that Ambassador Crocker's health has been poor for some time and the people who care about him most—his family, his friends and colleagues in the Foreign Service, and our Secretary of State herself—told Ambassador Crocker long ago that he needed to leave his post and that he needed to get away from the long days and long nights of too much stress and not enough sleep. They told him to come home for his own sake.

Eventually, Ambassador Crocker relented, but still he was only going to leave on his own terms. He said that America asks the best of our country—our men and women in uniform and their many civilian partners who work and sacrifice shoulder to shoulder with our troops in the field—to serve in Afghanistan for 1 year. Ambassador Crocker said he would expect no less of himself, and do no less, whatever the cost. So for the past few months, Ambassador Crocker has fought through persistent pain and discomfort to finish out his 1-year in Kabul, doing everything that is asked of him—and more. On Tuesday, that year came to an end, and Ambassador Crocker came home to receive the care he desperately needs.

This is a remarkable story, but it is only surprising to those who do not know Ryan Crocker. For those of us who have had the pleasure and the honor of coming to know Ryan well, this latest story is not at all surprising. It is actually quite in keeping with the character and the actions of this superb, decent, and selfless man—a man whom I would call, without question or hesitation, the most excellent Foreign Service officer and one of the finest public servants I have ever known.

For the past 41 years, ever since he was a junior diplomat serving in prerevolution Iran, Ryan Crocker has consistently answered the call to serve in the most challenging, the most difficult, but also the most important posts in the world. They were the places, as it turned out, where America needed Ryan Crocker the most, and he has always served with distinction.

He was a young officer in Lebanon when our Embassy was bombed, and Ryan Crocker helped to pull his colleagues from the rubble and then got back to work. He was one of the first civilians into Afghanistan and Iraq after the recent wars, helping to reestablish our diplomatic presence in both countries after decades. He returned to Iraq during the surge and, as General Petraeus tells everyone, was absolutely indispensable in turning around our war effort, even as his life was constantly in danger from the rockets that smashed into his office in Baghdad and, perhaps more threatening, his own relentless work ethic, which literally almost killed him.

Many Presidents, Republicans and Democrats alike, have had the wisdom to appoint Ryan Crocker as their Ambassador to six different countries—Lebanon, Kuwait, Syria, Pakistan, Iraq, and finally Afghanistan.

Ambassador Crocker has been just as indispensable in Kabul as he has everywhere else in his career, from enhancing our relationship with President Karzai and the people of Afghanistan, to negotiating and concluding the Strategic Partnership Agreement with Afghanistan, to being the dedicated partner every hour of every day of GEN John Allen and all of our men and women serving in harm's way.

In my many years and my many travels, I have had the pleasure and honor of meeting and getting to know many of our career diplomats, and I am continually impressed by their high quality and tough-mindedness, their patriotism and love of their country, their constant willingness to serve and the many quiet sacrifices they make. But of all of these remarkable men and women, never have I met a Foreign Service officer more outstanding or more committed to our country than Ryan Crocker.

The one comfort I take in Ryan's departure from Afghanistan is that he remains an abiding inspiration to his fellow diplomats, who revere him and hold him in the highest regard and wish to model themselves and their careers after his life and service. America will be a better and safer place because of this, thanks to Ryan Crocker.

Mr. President, I rise today to oppose the Cybersecurity Act of 2012 because it would do very little to improve our country's national security. In fact, in its present form, I believe the bill before us would do more harm to our country's economy and expand the size and influence of the Federal Government—specifically, the Department of Homeland Security—than anything else.

But before I begin my critique of the Cybersecurity Act, I would like to reaffirm my sincere respect for the lead sponsor of this bill—both sponsors, actually, both Senators LIEBERMAN and COLLINS. Although I disagree, whatever criticisms I may have with the legislation should not be interpreted as an attack on the sponsors of the bill but, rather, on the process by which the bill being debated today arrived before us and its public policy implications.

Consider this for a moment: If we pass this bill in its present form, which I hope we will not, we will have handed over one of the most technologically complex aspects of our national security to an agency with an abysmal track record, the Department of Homeland Security. The problems at DHS are too numerous to list here today, but I think I speak for many when I question the logic of putting this agency in charge of sensitive national security matters. They cannot even screen airline passengers without constant controversy. And do not forget that this is the same outfit in charge of the Chemical Facility Anti-Terrorism Standards Program, or CFATS, which was described in a recent report as ''at

measurable risk,'' beset by deep-seated problems such as wasteful spending and a largely unqualified workforce that lacks ''professionalism.'' I for one am not willing to take such a broad leap of faith and entrust this complex area of our national security and so many vibrant parts of our economy to this ineffective, bloated government agency.

The poor quality of the bill before us is a direct reflection of the lack of a thorough and transparent committee process. Had this bill been subjected to the proper process, my colleagues and I and the American public would have a much better understanding of the real implications of this undertaking. Unfortunately, this bill has not been the subject of one hearing, a single markup, or a whiff of regular legislative procedure.

Our Nation's cybersecurity is critical, and the issue is deserving of the regular order and the full attention and input of every Member of this body. I urge the majority leader to allow a full, fair, and open amendment process if cloture is invoked on the motion to proceed.

All of us should recognize the importance of cybersecurity. Time and again we have heard from experts about the importance of maximizing our Nation's ability to effectively prevent and respond to cyber threats. We have all listened to accounts of cyber espionage originating from countries such as China, organized criminals in Russia, and the depth of the threat from Iran in the aftermath of the Stuxnet leaks originating from the current administration. Unfortunately, this bill would do little to minimize those threats or generally improve our current cybersecurity posture.

The reason for this bill's general inadequacy is that rather than using a liability protection framework to enter into cooperative relationships with the private sector, which happens to own 80 to 90 percent of the critical cyber infrastructure in this country, this bill chooses to take an adversarial approach, with government mandates and inadequate liability protections.

Further, this bill includes unnecessary items that our government cannot afford and makes no mention of what the additional programs will cost. For instance, I am sure some of us have fond childhood memories of going to or taking part in a talent show, but to include talent show provisions in this bill is ridiculous. Title IV of this bill authorizes 9th to 12th grade cyber talent shows and cyber summer programs for kindergartners to seniors in high school—again, ridiculous, especially considering that the majority leader deemed this bill more important than the National Defense Authorization Act.

While I have criticisms with every title of this bill, I will limit my comments today to title I, which regulates critical infrastructure, and title VII, which concerns information sharing among the government and the private sector. In my view, these titles, along with weighing how much this bill, which lacks a CBO score—we do not even know how much it is going to cost—will ultimately cost and how it will dramatically increase the size of the Federal Government, are the most important aspects we can discuss.

With respect to the first title, title I, the proponents of the Cybersecurity Act would have you believe this bill authorizes the private sector to generate their own standards, that those standards are voluntary, and that the bill establishes a ''public-private partnership.'' Unfortunately, I disagree with each of those characterizations. As the bill is currently written, the government and not the private sector would have the final say on what standards look like and the private sector would be forced to comply. While my colleagues might suggest that section 103 states that the private sector proposes ''voluntary'' cybersecurity practices to the government, I call your attention to the following provision in section 103, which states the government would then decide whether and how to ''amend'' or ''add'' to those cybersecurity practices. Additionally, there is no recourse for the private sector to challenge the government's actions.

Soon after the government's takeover of the development of cybersecurity standards, any notion of the standards being ''voluntary'' evaporates. Section 103 clearly states: ''A Federal agency with responsibilities for regulating the security of critical infrastructure may adopt the cybersecurity practices as mandatory requirements.'' That is the language of the bill. What is being portrayed as ''voluntary'' proposals would soon become mandatory requirements.

Unfortunately, the conversion from voluntary to mandatory does not stop there. Shockingly, under this bill, if an agency does not adopt mandatory cybersecurity practices, it must explain why it chose not to do so. That is right. Under this bill, if a regulatory agency chooses not to mandate the ''voluntary'' practices, it must explain itself—as if it must be doing something contrary to the final objective. If this provision does not reveal the true regulatory intent of the proponents of this bill, nothing does.

Section 105 brings home this point by stating: ''Nothing in this title shall be construed to limit the ability of a Federal agency with responsibilities for regulating the security of critical infrastructure from requiring that the cybersecurity practices developed under section 103 be met.'' I would very much commend my colleagues to read that provision of the bill. All you have to do is read it. The regulatory result of these standards could not be clearer.

Moving on to title VII, which deals with the flow of information between the government and the private sector, the current bill is a step in the wrong direction. Specifically, the bill would make us less safe by failing to place the agencies with the most expertise and that are the most capable of protecting us on the same footing as other entities within the Federal Government. It strikes me as counterintuitive to prevent the institutions most capable of protecting the United States from a cyber attack and leave us reliant on agencies with far less capabilities.

Because this bill fails to equitably incentivize the voluntary sharing of information with all of the Federal Government's cyber defense assets, it does a great disservice to our national security. In cyber war, where speed and reaction times are essential to success, real-time responses are essential. The bill language states that information should be shared in ''as close to real time as possible.'' That may sound nice, but it will not get the job done.

We all agree that the threat we face in the cyber domain is among the most significant challenges of the 21st century. It is reckless and irresponsible to rebuild the very stovepipes and information-sharing barriers that the 9/11 Commission attributed as responsible for one of our greatest intelligence failures.

Because of my opposition to this bill and the lack of a regular legislative process, I have joined with Senators CHAMBLISS, HUTCHISON, GRASSLEY, MURKOWSKI, BURR, JOHNSON of Wisconsin, and COATS in offering an alternative cybersecurity bill. The fundamental difference in our alternative approach is that we aim to enter into a truly cooperative relationship with the entire private sector through voluntary information sharing rather than an adversarial one with the threat of mandates. Our bill, which also addresses reforming how the government protects its own assets, sets penalties for cyber crimes, refocuses government research toward cybersecurity, and provides a commonsense path forward to improve our Nation's cybersecurity defenses with no new spending. We believe that by improving information sharing among the private sector and the government, updating our Criminal Code to reflect the threat cyber criminals pose, reforming the Federal Information Security Management Act, and focusing Federal investments in cybersecurity, our Nation will be better able to defend itself against cyber attacks.

Even though we do not offer talent shows or summer camps in our bill, it has the support of the industries that themselves are under attack. Before I close, I would like to leave with you a final point which gets to the heart of why we are having this debate. In our country, unlike other countries around the globe, the private sector owns 80 to 90 percent of the critical cyber infrastructure.

This is a fact in which we should all take great pride. After all, it speaks to the essence of American entrepreneuralism and our spirit of individualism. The companies that own these systems are large and small, they

employ men and women everywhere, and their influence reaches every State, every congressional district, and about every corner of our country. While we all agree we are involved in a serious national security discussion, we must not forget to weigh the economic realities of this debate too.

I caution all my colleagues to tread very carefully because I am deeply concerned we are on the cusp of granting the Federal Government broad authorities and influence over one of the most vibrant and innovative sectors of our economy. The technology sector and the use of the Internet by American companies to innovate and improve the customer experience are deeply threatened by the heavy and too often clumsy hand of government.

As we confront the security challenges of an innovative economy, we must be careful not to undermine the economy itself. It is well known that we continue to have discussions amongst various parties: Senator KYL, Senator WHITEHOUSE, Senator LIEBERMAN, Senator COLLINS. Sometimes the crowd is large, sometimes it is not so large. I think we have made some progress. I think there is a better understanding of both of the different proposals that are before us. I do believe it is important, I do believe it is very important that businesses large and small in the United States of America, whether they be the utility companies or whether they be the most high-tech sectors, be represented in these discussions. We have tried to do that.

I believe we can make progress. I believe we can reach an agreement. I also know we have had several meetings and have not had extremely measurable progress. But I am committed to doing everything I can to see we reach that agreement before we conclude the consideration of this legislation.

I would also like to point out to my colleagues that I have had numerous conversations with my friends on the other side of the Capitol. They find this legislation in its present form unacceptable. I would hope we would also consider the fact that we need to get a final bill, not just one passed by the Senate.

I yield the floor.

The PRESIDING OFFICER (Mrs. HAGAN). The Senator from Illinois.

Mr. DURBIN. Madam President, consider these ominous words:

> To the loved ones of the victims who are here in this room . . . to those who are watching on television, your government failed you. Those who you entrusted with protecting you failed you. And I failed you. We tried hard, but that doesn't matter, because we failed.

Those are not my words. They contain a sentiment I hope none of us ever has to convey to the American people. Those are the words of Richard Clarke, the senior White House official who was in charge of counterterrorism efforts in the previous administration when the September 11 terrorist attacks occurred.

Mr. Clarke's testimony before the 9/11 Commission was apologetic, remorseful and tragic because he knew, he knew like no one else, our government had failed, failed to act on repeated warnings. This failure led to 9/11 and the largest loss of life on American soil at the hands of a foreign enemy since December 7, 1941, at Pearl Harbor.

Today, the national alarm security bells are ringing once again. This time, however, the enemy is not in a terrorist training camp learning how to make an explosive device or commandeer an aircraft. The enemy is not trying to sneak its way into the United States. The enemy we face does not need to hijack an airplane in order to wreck the American economy and to cause widespread loss of life. The only tool this enemy needs is a computer and access to the Internet.

The threat our Nation faces from a cyber attack will soon equal or surpass the threat from any terrorism that has consumed our attention so much since September 11. That is not my assessment. That is the assessment of the Director of the Federal Bureau of Investigation, Robert Mueller. In fact, he is not alone. There is an overwhelming bipartisan consensus among officials in the intelligence, defense, and national security community that America is incredibly vulnerable to a cyber attack that can be launched at any moment from anywhere in the world.

Michael Hayden, the former Director of the National Security Agency, Michael Chertoff, the former Secretary of Homeland Security who served under President George W. Bush, agreed. They and many other officials have joined the current Secretary of Homeland Security, Janet Napolitano, the current Director of the National Security Agency, GEN Keith Alexander, and others in warnings as follows: The cyber threat is imminent to America. It poses as serious a challenge to our national security as the introduction of nuclear weapons in the global debate 60 years ago.

The experts are sounding the alarm, telling us to take action now to prevent a catastrophic cyber attack that could cripple our Nation's economy, cause widespread loss of life, sadly send our economy into free fall. When the Cybersecurity Act of 2012 comes up for a vote, the Senate will have an opportunity to take action on this critical bill that will enhance our national security. In light of these warnings from the experts, the least we can do in the Senate is to vote to open the debate on this critically important bill.

I wish to thank its sponsors: Senator LIEBERMAN, the chairman of the subcommittee, Senator COLLINS, the ranking member, Senator FEINSTEIN of the Intelligence Committee, Senator ROCKEFELLER on the Commerce Committee. They have put a lot of time and effort into this important piece of legislation. They have worked together on a bipartisan basis. They have listened to a wide range of comments, including a few I have offered, and I am pleased the revised Cybersecurity Act of 2012 incorporates many suggestions.

It will help make America safe by enhancing our Nation's ability to prevent, mitigate, and rapidly respond to cyber attacks. The bill contains important provisions for securing our Nation's critical infrastructure. Every day, without thinking about it, we rely on powerplants, pipelines, electric power grids, water treatment facilities, transportation systems, and financial networks to work, to live, to travel, to do so many things we take for granted.

All those critical systems are increasingly vulnerable to cyber attack from our enemies. Last year, there was a 400-percent increase in cyber attacks reported by the owners of critical infrastructure, according to the Department of Homeland Security. That increase does not even account for the many attacks that went unreported.

We do not think twice about it, but this infrastructure is the backbone of America's economy and our way of life. This bill has provisions that will help minimize our vulnerability and shore up our defenses. The bill also includes a new framework for voluntary information sharing so government agencies and private companies can improve their mutual understanding of cyber threats and vulnerabilities and develop good practices to keep us safe.

I thought it was worth doing a few months ago to call together a dozen major corporations in Chicago and across Illinois that I thought, with the advice of some people who were experts, might be vulnerable to cyber attack. I asked those experts in a closed setting, outside the press, what Congress could do to help them secure their infrastructure at their business and networks from cyber attacks.

The answer from each and every one of them was the same: We need to be able to share information on cyber threats with the government and other private entities. We need to receive information from them in order to know what they have done to effectively prevent and mitigate attacks.

Estimates are that 85 percent of America's critical infrastructure is owned by the private sector. Since we depend so much on the private sector for our critical infrastructure, the lines of communication between government and the private sector must be open. If we share best practices, the result could be to make us a secure nation.

Let me say as well, I have the highest regard for my friend and colleague Senator JOHN MCCAIN of Arizona. Senator MCCAIN's life story is a story of patriotism and commitment to America. He understands the military far better than I ever will, having served and spent so many years working on the House Armed Services Committee. But I take exception to one of his statements earlier, at least what I consider to be the message of that statement, about how we have to be extremely careful in how we engage the

private sector in keeping America safe from cyber attack.

I believe we should be open, transparent, and we should be respectful of the important resources and capacity of the private sector. But I think back 70 years now to what happened in London, when there was a blitzkrieg, and the decision was made by the British Government to appeal to every business, every home, every family, every individual to turn out the lights, because if the lights were on, those bombers from Germany knew where the targets could be found. It was a national effort to protect a nation. Should it have been a voluntary effort? Should we have had a big town meeting and said: Some of you can leave your lights on if you like, if you think it might be an inconvenience.

There comes a moment when it comes to national defense when we need to appeal to a higher level in protecting America. My experience has been that the private sector is right there. They are as anxious to protect this country as anyone. They are as anxious to protect individuals, families, even their own businesses. So this notion that somehow we are adversarial in protecting America with the private sector I do not think is the case.

In fact, Senator COLLINS is here representing the other side of the aisle. I know it is not the case. She and I have worked together. I have been very respectful of the efforts she and Senator LIEBERMAN put into rewriting the rules for our intelligence community. They did it in a thoughtful and balanced way. This bill does too.

Are there amendments we might take? Of course. This is not perfect. No product of legislation is. But I have to say I believe the private sector will be our ally, our friend, our partner in making America safe. This should not be a fight to the finish as to whether it is government or the private sector which will prevail. Ultimately, America has to prevail.

Let me say a word about one part of this bill that I played a small role in addressing. Even through the threat in cyberspace is new and emerging, it calls to the forefront a familiar attention which we witnessed in Washington; on the one hand a mutually shared goal of protecting our country, on the other hand an important obligation to safeguard constitutionally protected rights to privacy and civil liberties.

It is this tension that led us to a conversation about some provisions and trying to find the right balance. The Cybersecurity Act of 2012 is not perfect, but it effectively strikes that balance between national security and individual liberty. The bill will enhance our national security and still do it in a way that is far superior to some of the alternatives that will be offered on the floor.

CISPA, the cybersecurity act that was passed by the House of Representatives, and SECURE IT, the alternative approach that has been introduced in the Senate, do not meet this standard, by my estimation. I wish to thank Senator COLLINS, Senator LIEBERMAN, and all those engaged in this conversation but special thanks to my colleague Senator FRANKEN because he is chair of the Privacy Subcommittee of our Senate Judiciary Committee.

We joined together with some colleagues: Senators COONS, BLUMENTHAL, SANDERS, and AKAKA. We asked the sponsors of the legislation to work with us and they did. The revised bill now requires that the government cybersecurity exchange, to which private companies can send threat indicators, must be operated by civilian agencies. I think that is smart.

The cybersecurity threat indicator could be a sensitive, personal communication, such as an e-mail from a spouse or private message on a social media site. As a result of our efforts, no longer can personal communications be indiscriminately sent directly to the NSA or CIA. The people who work at these agencies are fine, dedicated public servants, but these agencies are often shrouded in secrecy. I learned that as a member of the Senate Intelligence Committee.

To have the appropriate oversight, we ask that the first line of review be with a civilian agency subject to congressional oversight. This does not mean our intelligence and defense agencies will never be able to apply their experience and expertise to analyze and mitigate cyber threats. They should not be the first recipients, but the bill requires—and I think it is entirely appropriate—relevant cyber threat information can be shared by these agencies in real time. Waste no time doing it. Send it to the agencies if there is any perceived threat to America's security.

The revised bill no longer provides immunity for companies that violate the privacy rights of Americans in a knowing, intentional, or grossly negligent way—not simple negligence but things that go over that line dramatically.

I can support providing immunity for companies to share cybersecurity threats with the government, as long as they take adequate precautions and follow commonsense rules established in the bill.

The revised bill enables law enforcement entities to receive information about cyber crimes from cybersecurity exchanges without first going to court to obtain a warrant. To ensure these exchanges are not used to circumvent the Constitution and they do not create a perpetual warrantless wiretap, the bill requires law enforcement to only use information from the exchanges to stop cyber crimes, prevent imminent death or bodily harm to adults or prevent exploitation of minors.

The revised bill now requires that the rules for how the government will use and protect the private information it receives must be in place before companies begin sending information to the new cybersecurity exchanges. That makes sense. To be sure that government agencies follow the rules for using and protecting private information, the revised bill gives individuals the authority to hold the government accountable for privacy violations.

To ensure transparency and accountability, the revised bill requires recurring, independent oversight by the inspector general and the Privacy and Civil Liberties Oversight Board.

These are commonsense reforms. Senator LIEBERMAN spoke to the Democratic Senate caucus luncheon the other day and addressed these directly. He said he took these changes to those who were in charge of our cybersecurity and said to them: Give me an honest, candid assessment. If you think this ties our hands in protecting America, tell me right now. They reviewed them carefully, debated them, and came back and said: No, these are things we can live with and work with. That is the kind of approval we are looking for from those who have this awesome responsibility.

So as a result, this bill will have my support, because I think it keeps America safe from a threat which many Americans don't even know about but could literally take or change our lives in a heartbeat. It also has the support of many progressive groups from the left and center and right. It is an indication to me we have struck the right balance.

I thank those who helped us reach this point. As with any piece of substantial legislation, there is going to be disagreement. Senator MCCAIN expressed some areas of concern. That is what debate and amendments are all about. Let's move this bill forward this afternoon. Let's entertain relevant, germane amendments. Let's take this as seriously as the threat is serious to the United States. That, to me, is the right way to go.

Again, I thank Senator COLLINS personally and all the others who made this bill a reality in bringing it to the floor for our consideration.

I yield the floor.

The PRESIDING OFFICER. The Senator from Maine.

Ms. COLLINS. Madam President, I want to rise very briefly—I know there are a number of Members who are seeking recognition—to thank my friend and colleague from Illinois for his statement today. He has worked very hard on this bill. I know it is an issue he cares deeply about, and I very much appreciate his taking the time to come to the floor and to urge Members to vote for the motion to proceed to the debate on this absolutely vital piece of legislation.

I must say I was disappointed to hear some of the comments made on the Senate floor today in opposition to this bill. The fact is both Republican and Democratic officials have, with very

few exceptions, endorsed the framework of this bill and urged us to move forward. In fact, they have warned us repeatedly in saying the only question is when a major cyber attack will occur. Not whether it will occur, but when it will occur. We have letter after letter, statement after statement from national and homeland security experts, representing both President Bush's administration and the current administration, urging us to act.

Indeed, yesterday the Aspen Institute Homeland Security Group put out a statement, stating the following:

The Aspen Homeland Security Group strongly urges the U.S. Senate to vote this week to take up S. 3414, the cyber-security bill, for debate on the Floor.

The statement goes on to say:

We urge the Senate to adopt a program of voluntary cyber-security standards and strong positive incentives for critical infrastructure operators to implement those standards. The country is already being hurt by foreign cyber-intrusions, and the possibility of a devastating cyber-attack is real. Congress must act now.

This letter is signed by officials from the previous administration, such as Charles Allen, Stewart Baker, Michael Leiter, and Michael Chertoff. There are numerous representatives of past administrations and individuals who are renowned for their expertise. How can we ignore their warning that we must act, that it is urgent, and that we must have voluntary standards for critical infrastructure—infrastructure that, if it were attacked, would result in mass casualties, mass evacuations, a severe blow to our economy, or a serious degradation of our national security?

That is the definition of the core critical infrastructure we want to cover and to help make more secure through a partnership with the private sector. And it has to be a partnership because 85 percent of critical infrastructure is owned by the private sector. We have worked hard to alter our bill to take suggestions from the private sector, from our colleagues, from the administration, and from experts across the philosophical range to improve our bill.

I heard a Member saying this morning that somehow we are going to be hurting the high-tech sector of our society. Well, that is not what Cisco and Oracle think—certainly two of the leading businesses in the high-tech sector. This morning they wrote to us, the chief sponsors of the bill—Chairman LIEBERMAN, Chairman ROCKEFELLER, Chairman FEINSTEIN, myself, and Senator CARPER—and I want to read a brief excerpt from their letter. They said:

. . . we appreciate your efforts to craft legislation that addresses the important issue of cybersecurity by supporting American industry in its efforts to continue to be the world's leading innovators.

The fact is, it is American businesses that are being robbed of billions of dollars every year due to cyber intrusions from foreign governments, from transnational criminals, and from hackers. This is a threat not only to our national security but to our economic prosperity.

That is why the letter from Cisco and Oracle goes on to say:

We praise your continued recognition of the importance of these objectives through the provisions of S. 3414.

They say they support those provisions. Continuing to read from the letter:

We also commend your commitment to ensuring that the IT industry maintains the ability to drive innovation and security into technologies and the network.

So the idea we heard this morning on the Senate floor that somehow we are going to bring innovation in America to a standstill or hurt this important sector of our economy is not supported by a reading of our bill, and it is certainly contradicted by the letter we received from Cisco and Oracle, leading companies in the high-tech sector.

Finally, I would point out they thank us for our outreach, our willingness to engage in an exhaustive process around this issue set, and to consider and to respond to the views of America's technology sector. That is what we have done. That is what we are continuing to do with our colleagues on both sides of the aisle who bring varying views to this issue. But what we cannot do is to fail to act when the warnings are so constant and alarming about the threats to our Nation, to our economy, and to our way of life.

Madam President, I ask unanimous consent to have printed in the RECORD the statement from the Aspen Institute Homeland Security Group as well as the July 26 letter from Cisco and Oracle.

There being no objection, the material was ordered to be printed in the RECORD, as follows:

JULY 24, 2012.

STATEMENT OF THE ASPEN HOMELAND SECURITY GROUP

The Aspen Homeland Security Group strongly urges the U.S. Senate to vote this week to take up S. 3414, the cyber-security bill, for debate on the floor. We urge the Senate to adopt a program of voluntary cybersecurity standards and strong positive incentives for critical infrastructure operators to implement those standards. The country is already being hurt by foreign cyber-intrusions, and the possibility of a devastating cyber-attack is real. Congress must act now.

Charles E. Allen; Stewart A. Baker; Richard Ben-Veniste; Peter Bergen; Michael Chertoff; P.J. Crowley; Clark K. Ervin; Jane Harman; Michael V. Hayden; Michael Leiter; James M. Loy; Paul McHale; John McLaughlin; Phillip Mudd; Eric T. Olson; Guy Swan, III; Juan Zarate; Philip Zelikow.

JULY 26, 2012.

Hon. JOSEPH I. LIEBERMAN,
Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.
Hon. SUSAN M. COLLINS,
Ranking Member, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.
Hon. JOHN D. ROCKEFELLER,
Chairman, Committee on Commerce, Science and Transportation, U.S. Senate, Washington, DC.
Hon. DIANNE FEINSTEIN,
Chairman, Select Committee on Intelligence, U.S. Senate, Washington, DC.
Hon. THOMAS R. CARPER,
U.S. Senator,
Washington, DC.

DEAR SENATORS LIEBERMAN, COLLINS, ROCKEFELLER, FEINSTEIN AND CARPER: As two of the industry-leading companies providing information technology across the nation and the world, we appreciate your efforts to craft legislation that addresses the important issue of cybersecurity by supporting American industry in its efforts to continue to be the world's leading innovators. This matter deserves the continuing attention of industry, the Congress and the Administration, and we commend you for having constructively engaged stakeholders throughout this process.

As you know, effective cybersecurity must be driven by an IT industry that is free to drive innovation and security and maintain world leadership in the creation of secure systems. Effective cybersecurity depends on our having the ability to drive innovation globally—it is our core value. We have long advocated a cybersecurity approach based on the importance of real information sharing that can help protect important assets. We thank you for your leadership in recognizing that any cybersecurity legislation must incorporate iron-clad protections to ensure American industry remains the world's leader in the creation and production of information technology, and to make certain that legislation maintains and protects industry's ability and opportunity to drive innovation and security in technologies across global networks.

We praise your continued recognition of the importance of these objectives through the provisions of S. 3414, the Cybersecurity Act of 2012. The provisions regarding the designation of critical cyber infrastructure, the specifics of cybersecurity practices, and the treatment of the security of the supply chain demonstrate your continued recognition of these core principles, and we support them. Wherever the important cyber debate takes this legislation, these core principles should be promoted and preserved. We believe these provisions as written capture that principle and believe it is in the interest of cybersecurity and critical infrastructure that they remain explicit. We also commend your commitment to ensuring that the IT industry maintains the ability to drive innovation and security into technologies and the network. Further, we appreciate the recognition that more needs to be done in advancing innovation through increased research and development, and in raising awareness and education, and importantly on increasing global law enforcement.

By explicitly maintaining these principles and provisions, your legislation proposes a number of tools that will enhance the nation's cybersecurity, without interfering with the innovation and development processes of the American IT industry. Ultimately, the ability of the tech industry to continue to innovate will provide the best defense against cyber attacks and data breaches.

We also note the shift toward a voluntary framework for critical cyber infrastructure in the new bill, and commend and support the great strides you have made toward that goal. We look forward to continuing to work with you on this issue.

We thank you for your outreach, willingness to engage in an exhaustive process around this issue set, and to consider and respond to the views of America's technology sector. We look forward to working with you and others in the Congress to continue the public-private collaboration and to make sure that what results continues to meet our common goals.

Sincerely,

BLAIR CHRISTIE,
Senior Vice President and Chief Marketing Officer, Government Affairs, Cisco Systems, Inc.
KENNETH GLUECK,
Senior Vice President, Office of the CEO Oracle Corporation.

Ms. COLLINS. Madam President, I yield the floor.

The PRESIDING OFFICER. The Senator from Minnesota.

Mr. FRANKEN. Madam President, I rise today to talk about our Nation's defenses against cyber attacks, and I wish to commend the Senator from Maine for her leadership. She is the ranking member, of course, on the Committee on Homeland Security and Governmental Affairs. I wish also to commend all three chairs, Senators LIEBERMAN, FEINSTEIN, and ROCKEFELLER, for their work.

As I said, I rise today to talk about our Nation's defense against cyber attacks and how our Nation needs to respond to those threats which affect our national security, our economic security, and our privacy.

News reports and experts confirm our Nation's critical infrastructure, such as our water systems, our power grid and so forth, are vulnerable to attacks from hackers and foreign governments. Every few weeks we hear about yet another breach—Yahoo and Gmail, Citibank, Bank of America, Sony PlayStation. Millions of people have had their names, passwords, credit card information or health information compromised.

It isn't just our national security or economic well-being that is being threatened by these attacks, it is the Internet itself. If you want to use Facebook or a cloud-based e-mail provider to communicate with your friends and loved ones, you need to know that your private communications won't be exposed by hackers. If you want to use the Internet to spread new ideas or fight for democracy, you need to know your work won't be disrupted by hackers or repressive regimes.

Unfortunately, it is hard to write a good cybersecurity bill, because when you try to make it easier for the government or Internet companies to detect and stop the work of hackers or other bad actors, you often end up making it easier—or very easy—for those same entities to snoop in on the lives of innocent Americans.

Until recently, every major cybersecurity bill on the table would have done too much to immunize and expand the authority of the government and industry and far too little to protect our privacy and civil liberties. These bills would make it too easy for companies to hand over your e-mails and other private information to the government—even to the military. Setting aside the fourth amendment, these bills would allow almost all of that information to go to law enforcement. And these bills do far too little to hold these companies and the government accountable for their mistakes.

A few months ago, I teamed up with Senators DURBIN, WYDEN, SANDERS, COONS, BLUMENTHAL, and AKAKA to try to address this situation. We worked with privacy and civil liberties groups on the left, the right, and the center to come up with a package of proposals. We worked with the ACLU, the Electronic Frontier Foundation, and the Center for Democracy and Technology, which are traditionally associated with progressives; we worked with the Constitution Project, which is a bipartisan centrist think tank; and we worked with TechFreedom and the Competitive Enterprise Institute, which are conservative libertarian organizations.

Together, we approached Chairman LIEBERMAN, Ranking Member COLLINS, Chairman ROCKEFELLER, and Chairman FEINSTEIN, and proposed a package of amendments to the information-sharing title of the Cybersecurity Act of 2012.

The information-sharing title is the part of the bill that will make it easier for companies to share critical information about cyber attacks with each other and with the government. These Senators engaged with us earnestly and in good faith. After a lot of hard work and a lot of conversations, the sponsors made a series of changes to the bill that are major, unequivocal victories for privacy and civil liberties.

The bill is still not perfect, from my point of view, but I can say with confidence that when it comes to protecting both our cybersecurity and our civil liberties, the Cybersecurity Act of 2012 is the only game in town.

I want to take a moment to explain the changes made to the information-sharing title, and compare how the Cybersecurity Act now stacks up with its rival bills, the Cyber Intelligence Sharing and Protection Act, or CISPA, which recently passed the House, and the SECURE IT Act, which has been introduced here in the Senate.

First of all, I agree we need to make it easier for companies to share time-sensitive information with experts in the government. But the cyber threat information that companies are sharing often comes from private, sensitive communications, like our e-mails. And so the gatekeeper of any information shared under these proposals should never be the military. It should never be the NSA. The men and women of the NSA are patriots and they are undoubtedly skilled and knowledgeable. But as Senator DURBIN said, that institution is too shrouded in secrecy. And—he didn't say but as I will say—it has too dark a history of spying on innocent Americans to be trusted with this responsibility under any administration.

Under the new, revised Cybersecurity Act of 2012, the one that will soon be before us on the floor, companies can use the authorities in the bill to give cyber threat information only to civilian agencies. That is a critical protection for civil liberties, and it is a protection that CISPA and the SECURE IT Act do not have. I want to be very clear. An America with CISPA and an America with the SECURE IT Act is an America where your e-mails can be shared directly, immediately, and with impunity, with the NSA.

Second, any cybersecurity bill should focus on just that—cybersecurity. It should not be a back door for warrantless wiretaps or information entirely unrelated to cyber attacks. In other words, once a company gives the government cyber threat information, the government shouldn't be able to say, Hey, this e-mail doesn't have a virus, but it does say that Michael is late on his taxes; I am going to send that to the IRS.

Under the Cybersecurity Act of 2012, once a cyber exchange gets information, it can give that information to law enforcement only to prosecute or stop a cyber crime or to stop serious imminent harm to adults or serious harm to minors. CISPA actually has similar protections, but SECURE IT allows a far broader range of disclosures to law enforcement. Here in the Senate, the Cybersecurity Act is the proposal that does the most to respect the spirit and letter of the fourth amendment.

Third, a cybersecurity bill should make it easier for a company to share information with experts in the government. But it has to hold companies that abuse that authority accountable for their actions. Both CISPA and the SECURE IT Act give companies immunity for knowing violations of your privacy. Under CISPA and the SECURE IT Act, if a company's CEO knows for a fact that his engineers are sending every one of your e-mails to the NSA, there is nothing you can do about it. That is not an exaggeration. Thanks to the changes I have pushed for—along with Senators DURBIN, WYDEN, COONS, SANDERS, BLUMENTHAL, and AKAKA—the Cybersecurity Act does not protect companies that violate your privacy intentionally, knowingly, or with gross negligence.

Fourth, and finally, a cybersecurity bill should also hold the government accountable for its actions. Under both CISPA and the SECURE IT Act, companies can start giving the Federal Government your private information well before the government actually has privacy rules in place for how to handle that information.

Under the SECURE IT Act, the government has total immunity from lawsuits arising out of its cybersecurity

operations—total immunity for the government. The SECURE IT Act also lacks any regular independent oversight of the Federal Government's actions under these new authorities. The Cybersecurity Act of 2012 now has all three of these protections. Under this bill, privacy rules have to be in place on the first day companies start giving the government information. People can sue the government when it abuses its authority. And there will be recurrent, independent oversight by both the Privacy and Civil Liberties Oversight Board and inspectors general.

These are just the four main categories of changes that the sponsors of the Cybersecurity Act have adopted. There are other changes, too, that I won't go into now.

Before I close, I want to elaborate on one way I do think we need to improve the Cybersecurity Act to better protect privacy. The sponsors of the bill have rightly adopted several critical protections. I hope they will accept at least one more amendment that I think is very important. I will talk about my amendment more on another occasion, but for now I want to flag it for my colleagues.

For decades, Federal law has given Internet service providers and other companies the right to monitor their systems to protect themselves and their customers from cybersecurity threats. They also have the right to deploy what are called countermeasures to protect their systems against those threats. So these companies have the right to monitor and protect themselves; but at the same time, Federal law prevents them from abusing those rights. If an ISP starts randomly picking customers and reading their e-mails, their customers—and the government—can take them to court, and the ISP can't throw its hands up and plead cybersecurity.

This is why, when the President of the United States brought together all of the Federal agencies to craft a bill that would comprehensively protect our cybersecurity, that proposal included a new authority for companies to disclose information to the government but contained no new authority for companies to monitor e-mail or deploy countermeasures. When the administration's lawyers were asked why that was, they said that doing so would have been duplicative—duplicative—because the companies already have those rights.

Right now, the Cybersecurity Act and the President's proposal are not in line with each other, because unlike the President's proposal, the Cybersecurity Act does give ISPs and other companies a brandnew right to monitor communications and to deploy countermeasures. That right is very broad—so broad that if a company uses that power negligently to snoop in on your e-mail or damage your computer, they will be immune from any lawsuit. I plan to offer an amendment to delete these new monitoring and countermeasures authorities and bring this bill in line with the President's proposal. I hope my colleagues here in the Senate will join me in passing this amendment. Seven of my colleagues have already indicated they will cosponsor this amendment.

But I want to end on a high note. I don't want my amendment to cloud my central message here, so I will repeat what I said earlier. The Cybersecurity Act is not perfect, but when it comes to striking a balance between cybersecurity and privacy and civil liberties, it is the only game in town. It is far more protective of our rights than either CISPA or the SECURE IT Act. I thank the sponsors of the Cybersecurity Act for taking this high road, and I urge my colleagues to vote to proceed to the bill so we can have a good, full debate on it.

Madam President, I yield the floor.

The PRESIDING OFFICER. The Senator from Delaware.

Mr. COONS. Madam President, I am honored to be able to join the Senator from Minnesota in speaking today in support of all the Members of this body voting to proceed to the consideration of the important cybersecurity bill to which he and Senator DURBIN have spoken.

Today we have an opportunity to celebrate progress—very real, very concrete, and very important progress—in the legislative efforts to make America both more secure and yet retain our core constitutional freedoms: the protections of privacy that Americans have held dear from the very beginning of this Republic.

As I have said before on this floor, taking action to protect our Nation from the very real and urgent threat of cyber attack is of paramount importance, something so urgent that it deserves our undivided attention. But so is protecting the privacy rights of lawabiding American citizens.

As we work together toward this commonsense, compromise piece of legislation the Senate should consider in coming days, I fought hard, along with several colleagues, to ensure we maintain the right balance between privacy and security. That balance is essential. Compromising our liberty would be as dangerous as compromising our safety. But thanks to the hard work of so many of my colleagues—in particular Senator DURBIN, Senator FRANKEN, Senator BLUMENTHAL, Senator MERKLEY, Senator SANDERS, and others—we found that appropriate balance in this legislation that is before us.

The changes we have made to the original text and to the House-passed version have significantly strengthened privacy rights. That is why I say we can celebrate real progress here today.

I long thought it was the privacy issues that would be the rock on which this ship would founder, that the critical and unaddressed privacy issues in CISPA and SECURE IT, spoken to by Senator FRANKEN, would be issues that would prevent me from supporting cybersecurity legislation in this session of Congress. But we have made remarkable progress. Let me briefly review a few of the areas where that progress has been made.

We made sure companies cannot pry into the private online activities of everyday Americans in the name of national security. I want to mention one more improvement.

In addition to those mentioned by Senator FRANKEN just before me concerning legal immunities contained in this bill, this bill appropriately gives companies the authority to share cyber threat-related information with each other and the government, without which we can't know what the rapidly emerging significant national cyber threats are. It also gives them immunity from suit if they do so. So if companies share with each other real-time cyber threat information, they cannot be sued. But prior versions of this bill might have provided bad actors with immunity against all privacy laws. So instead, we added tough provisions to ensure if a company acts recklessly or willfully to violate the law and the online privacy of its customers, they will be held accountable. This legislation now, in my view, strikes an appropriate balance between empowering companies and providing them certainty, as well as maintaining the privacy rights of Americans and their customers.

In this new, better, stronger legislation, it is no longer the case that companies can share your data and violate your privacy because you interact with them online. If that had remained in this bill, I would have expected millions of Americans to mobilize to stop this legislation. But we are here today as a group of Senators to announce that real progress has been made, and we are comfortable with and support this legislation from a privacy perspective.

I urge my colleagues, when we take up this vote later this afternoon, to vote to proceed to the bill and to allow us a full and robust debate on this cybersecurity legislation.

Getting to this new and improved legislation was a team effort, and special credit is due to Senators LIEBERMAN and COLLINS for leading the way, for being willing to find common ground on challenging issues. There was also a great deal of work done by my senior Senator TOM CARPER and by Senators FEINSTEIN and ROCKEFELLER who chair committees and were also essential to making such great progress.

One of the aspects of cybersecurity and the threat to our country that keeps me up at night is that it is constantly evolving. Our enemies are smart, they are capable, and they are fast. That means our cyber defenses have to be flexible, adaptable, and regularly evaluated in order to keep up.

One good thing about the House version of this legislation is that it includes a sunset provision requiring that in 5 years, this body once again

must take a hard and serious look at cybersecurity threats, and update or change our defense as needed, and ensure that privacy protections have been fully observed.

That is not just good strategy, it is good sense. Think about the capabilities of your computer, your cell phone 5 years ago compared to today. The pace of change is faster online than ever before, and we need the kind of legislative process that allows us to review our work and ensure not only that we stay ahead of the curve in defending our country but we continue to strike the right balance between privacy and security.

That is why, similar to Senator FRANKEN before me, I intend to introduce an amendment on the floor—which I hope will earn consideration by this body and the support of my colleagues—to take the sunset provision of our House counterparts and match that in the Senate in this bill. It is the right thing to do to help keep us safe and to help our military leaders and cybersecurity experts stay one step ahead of those who would wish us harm.

In closing, I thank Senator WHITEHOUSE, who has been an important part of two different teams working on this bill. Senators KYL and WHITEHOUSE led a team that worked hard on critical infrastructure. I wish to thank Senator BLUMENTHAL of Connecticut, who participated in the privacy side work and in the critical infrastructure work. Now we are speaking to title VII, to the information-sharing provision of the bill and the dramatic and real progress that has been made in addressing the balance between security and privacy.

There has also been great progress made, in my view, in addressing the issues of critical infrastructure, and I invite Senator BLUMENTHAL of Connecticut, who has contributed so well to both these efforts, to address the Chamber at this time.

I yield the floor.

The PRESIDING OFFICER (Mrs. MCCASKILL). The Senator from Connecticut.

Mr. BLUMENTHAL. Madam President, I thank my very distinguished and effective colleague from Delaware for his great work as part of a team that has sought to enhance the protections of privacy in this bill. His perspective as a local official, as a constitutional expert, as someone who cares deeply about privacy and civil liberties, has been invaluable to this effort. He too has participated in the critical infrastructure team which both of us have been privileged to join with Senators WHITEHOUSE and KYL, who have been so enormously helpful in this effort. I join him as well in thanking our colleagues Senators AKAKA, DURBIN, FRANKEN, SANDERS, and WYDEN for their very important efforts to protect privacy and civil liberties in the information-sharing title of the cybersecurity act.

We have truly worked as a team and, in many ways, a bipartisan team in forging this legislation. Of course, we have followed the lead of Senators LIEBERMAN and COLLINS who have been at the forefront of this effort, as well as Senators ROCKEFELLER, FEINSTEIN, and CARPER, who deserve our appreciation for drafting the bill, shepherding it through committee, and bringing a modified version to the floor where now we have the historic opportunity to move forward. I am here to urge my colleagues, in fact, to move forward and vote to proceed to the bill later today.

We have made good progress on this legislation. I am optimistic that we will pass a cybersecurity bill in the very near future—as we must for all the reasons that have been articulated by myself and others. This Nation is under attack. It is under cyber attack. Literally, every day our defense industrial base, our military systems, and our private industry are under attack by nations and by hackers, both sophisticated and unsophisticated, abroad and at home. We must make sure we provide the tools and the resources, legal resources and authority to stop that attack, to deter it, to defeat it, to make sure our country is defended against it effectively and comprehensively.

The nature of defending against cyber attack involves information sharing. There is no way around that basic fact that information about the attacks—the sources, the objects and targets, the times—all the details are, in essence, the power to defend. Information is power when it comes to defending against cyber attack. Yet we also know that information, when shared, can also be abused. Some of the most tragic chapters of our Nation's history have involved snooping, spying, surveilling, and then sharing of information that is inappropriate and unnecessary and sometimes illegal.

We know also that one of our core constitutional protections is, in fact, the right to privacy. It is enshrined in our Constitution. It dates from our founding. It is integral to the fabric of the rule of law. We resisted and rejected the rule of the British, in part, because they had no respect for the privacy of the colonials. That basic value has inspired the rule of law since.

There is a saying—I believe it is a Latin saying—that in war, law is the first casualty. We are in a cyber war, but our constitutional law cannot be a casualty. Our right to privacy and civil liberties must be protected.

Information sharing must involve the right information shared with the right people and officials for the right purposes. There must be red lines and red lights. There must be consequences if those red lines or red lights are disregarded or dismissed.

This bill meets those basic requirements. It is enforceable and it must be enforced. In fact, I will offer an amendment to increase the enforceability and enforcement of these basic protections by increasing the penalties for violating these basic protections. The trust and confidence of our Nation in the rule of law depends on our getting it right: information sharing with the right information to the right people and for the right purposes.

The kinds of modifications contained in this bill are critically important. They are in sharp contrast to the House-approved version of CISPA, which utterly fails to protect civil liberties and privacy rights in sufficient degree. Unlike past versions, this measure establishes unequivocal civilian control of cybersecurity information exchanges. Unlike past versions, this bill bars companies from using cybersecurity as a pretext for violating FCC net neutrality rules. Unlike other versions, this bill bars companies from using cybersecurity as a pretext for violating other guarantees, and it allows citizens to hold companies accountable and take them to court for knowingly or grossly negligent violations of the information-sharing provisions of this bill.

Equally important, it enables them to hold the U.S. Government and other public officials responsible and take them to court if they violate the privacy guarantees in this bill.

A private company receiving someone's private information while monitoring for cyber threat should protect that information. It is a public trust and a public responsibility. This act protects Americans' privacy by requiring companies that obtain that kind of information—some of it medical or financial of the most confidential and private nature—through monitoring, to protect that information.

This measure also imposes restrictions on the use of shared information for law enforcement purposes. The government can only provide information to law enforcement if it relates to a cyber crime or a serious threat to public safety; that is, physical safety—bodily harm. Law enforcement can only use information to prosecute or stop cyber attacks to prevent that kind of imminent and immediate harm to a person or a child.

There are other protections—some of them have been mentioned by Senators FRANKEN and COONS before me—that I will support. For example, Senator FRANKEN mentioned that his amendment would eliminate new authorities in the bill to monitor communications or operate countermeasures. Senator COONS mentioned a 5-year sunset on the use of information sharing under this measure to help guard against unforeseen consequences of the legislation and ensure that congressional oversight occurs on a regular and foreseeable basis. Other measures which I consider important would require Federal agencies that suffer a data breach to notify affected individuals and allow those individuals to recover damages and require the creation of a new office in the Office of Management and Budget, that of Chief Privacy Officer.

I support these amendments and I support also increasing the penalties in the event that government or companies violate the protections in this statute.

We have indeed made progress. There is more to do. I hope more progress will be made. I foresee passage of a cybersecurity measure that is desperately and direly needed in this country—not at some point in the future but now. As others before me have said on this floor and as I have said before, cybersecurity is national security and we must protect our national security while at the same time retaining the reason, our fundamental rights and civil liberties, that we want to protect our Nation and its constitutional values.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The assistant legislative clerk proceeded to call the roll.

Mr. MORAN. Madame President, I ask that the order for the quorum call be rescinded and that I may speak as in morning business.

The PRESIDING OFFICER. Without objection, it is so ordered. The Senator may speak as in morning business.

MEATLESS MONDAY

Mr. MORAN. Madam President, yesterday I was on the Senate floor, and I had the opportunity to highlight a development at the Department of Agriculture. We learned yesterday afternoon that the Department of Agriculture, in an employee newsletter, was promoting something called Meatless Mondays. The Department of Agriculture newsletter offered encouragement for its employees and I assume others who might see the newsletter—even tourists who visit Washington, DC, and eat at the Department of Agriculture cafeteria—to participate in Meatless Monday. It indicates the desirability of reducing the consumption of meat and dairy products. I found that very startling and surprising. Never in my life would I expect the Department of Agriculture, which I always presumed is the farmers' and ranchers' friend, to be promoting the idea that it is a bad idea to eat the products of farms and ranches across Kansas and our Nation. Yet that is what we saw and read yesterday.

The Department of Agriculture newsletter said that ''beef production requires a lot of water, fertilizer, fossil fuels, and pesticides. In addition, there are many health concerns related to excessive consumption of meat.'' Those are the words of the Department of Agriculture newsletter. I am pleased to report that in asking Secretary Vilsack to reconsider what the Department had said and was promoting, they have done that and they have apparently removed the promotion from their newsletter and from their Web site. That is a positive development, and so I appreciate that happening.

It is amazing to me, unfortunately, that this is just one of many circumstances in which we see administration agencies and departments on the side of something that those of us who believe strongly in traditional family agriculture across the country believe is very important. One would expect in this case that the Department of Agriculture would promote the consumption of meat. In fact, within the Department of Agriculture, we have the Secretary saying in his mission statement that he is about increasing and expanding domestic and foreign markets for beef and meat products. We have the U.S. beef board, organized and monitored by the Department of Agriculture, whose job it is to promote agricultural products. Many of us in Congress try to encourage the sale of agricultural products, particularly meat and beef products, to South Korea and China. We have debated on the Senate floor the value of trade agreements, most recently with Colombia, South Korea, and Panama, because we believe in the opportunity for American producers to sell their products around the globe. Yet we saw at least some at USDA who have the view that we need to discourage the consumption of meat for environmental and health reasons.

Particularly troublesome is the fact that the Department of Agriculture was citing the United Nations as a reason that we ought to discourage the consumption of beef for environmental reasons. Our Department of Agriculture positions ought to be based upon sound science, not some U.N. study.

Beef is an important and vital component of the Kansas economy. We are the second largest beef-producing State in the country. The economic impact to our country is around $44 billion. Beef exports in 2011 were over $4.08 billion. This matters to us greatly.

This is happening at a time in which to the cattle producers across the Midwest, including in the State of the President today, the drought is so damaging.

It is also happening at a time in which we have been having the debate about the farm bill. My farmers in Kansas will often say: I know we need to do something about reducing spending. We have to get the deficit under control.

In fact, the farm bill we passed in the Senate has a reduction in the farm bill spending of $23 billion. No one likes to see something that is important to them go away, but if this farm bill becomes legislation and direct payments leave, the safety net for producers across our country will be less. Yet farmers and ranchers say: We have a responsibility as American citizens to give these things up, to reduce the spending that comes our way, but please don't do anything that is damaging to us as far as our ability to earn a living in the free market, in the real world.

So when we see something like this from the Department of Agriculture discouraging the use of meat products—and, again, at a time in which the temperatures across my State have been over 100 degrees for more than a month. We had a record high of 118 degrees. Perhaps that is a record high on the globe. It certainly is in the United States. In Norton, KS, it was 118 degrees. Rain is so scarce, we spend a lot of time in our State down on our knees praying for moisture and we spend a lot of time looking up to the skies hoping for moisture. We need to make sure that what we do in this Congress and what the Obama administration does is not something that diminishes the chances for the survival of family farms in the United States, certainly at home in Kansas and around rural America.

If this was just an isolated instance, perhaps the point has been made and the words have been withdrawn, but I remember we started a year ago with a Department of Labor that concluded that we need to regulate the use of 14- and 15-year-olds on family farms. That was a real misunderstanding of how production agriculture and family farms work. Agriculture is a family operation, and yet we had the Department of Labor suggesting that someone 15 years old should perhaps not be able to work on their own family's farm. I remember just 6 months or so ago, I was on the Senate floor worried about a Department of Agriculture forum on animal safety that was being organized by the Humane Society. Again, my farmers and ranchers would say—particularly in a time of drought and where the safety net provided by the farm bill is going to become less—please don't do anything that is harmful to us, that reduces the chance for us to succeed.

In this regulatory environment in which we find ourselves, we need to take the steps that promote agriculture, not do things that diminish the opportunity for a farmer or rancher to earn a living in the free market.

Yesterday we had a debate about estate taxes and the consequences to family agriculture across the country, and again, at a time in which the drought is so prevalent, circumstances so difficult, the Tax Code matters greatly and the ability to pass a family farm from one generation to the next is critical. It is so much about agriculture in States such as mine that when our farmers and ranchers don't succeed, the success of the communities in which they live and raise their kids greatly diminishes. This is a way of life for us, and we need to make certain we have a Department of Agriculture that is promoting our farmers and ranchers and their success.

I was on the Senate floor yesterday with the Senator from Wyoming. We had a conversation about the drought, the estate taxes, and the farm bill. I am interested if the Senator from Wyoming has any further thoughts. I know he is a leader in the Western Caucus. As Members of the Senate, we are in

the process of writing Secretary Vilsack in regard to the promotion of Meatless Monday. There are those who have a different view about what their menus should be and what they want to see on the menu, and that is fine with me. That is a personal decision. But the Department of Agriculture ought to be supportive of the people who produce the food, fiber, and energy for our country each and every day. They get up at sunrise and go to bed after sunset because they are out there trying to make a living on family farms across the country.

I yield for the Senator from Wyoming.

Mr. BARRASSO. Madam President, never in my life would I expect to see the U.S. Department of Agriculture come out against farming, ranching, agriculture, and its products.

I was talking to a radio station this morning in Afton, WY. They were astonished. They had not heard the news of this yet, and they are now fully aware of it. They are grateful to the Senator from Kansas because one of those involved actually had heard the Senator on the floor last night talking about Meatless Mondays and then the USDA linking ranching and farming to climate change. It is not just cattle or beef producers—and beef is clearly the No. 1 cash crop for Wyoming—but the USDA has gone after dairy products, such as milk and cheese, as part of a climate change issue.

So this does seem to be an assault against a way of life, a significant part of our country's heritage, as well as our economic future. We see this assault on our products through the Department of Agriculture. We see it as an assault on family values of young families working together, as we have seen with the Department of Labor. And now yesterday, with a vote on this Senate floor, there was an attack by a reinstitution of the death tax. People are trying to keep a family operation within the family, a ranch or a farm, all across rural America. These small businesses in communities all across the country are finding that it is going to be much more difficult, under what the Democrats voted for yesterday, to keep their ranches and farms in the family.

I know farmers and ranchers in Wyoming where a member of the family works in town just to make the money to pay the expenses of keeping the operation of the farm or the ranch going. They know full well that under the Democratic proposal, if someone were to die, once that becomes the case, their chances of being able to hold on to that operation are reduced to almost nothing. Bringing back the costs of the death tax to the levels of the Clinton administration, anything over $1 million in assessed value would be taxed at 55 percent. The only solution for many is to sell.

There are three specific attacks: the death tax attack, the Meatless Monday attack, and the attack on children helping out on the family or neighbor farm or ranch. There are values that they learn through the FFA. All of those things make me wonder in what direction the country is heading. I guess that is no surprise when only one in three Americans all across the country think the country is heading in the right direction.

I am happy to join my colleague from Kansas who came to the Senate floor yesterday to bring this to the attention of the Senate. He and I are working together to now address the Secretary of Agriculture to make sure that something like this doesn't happen again and to make sure that the Secretary does insist that farmers and ranchers across this country—and the products that they make and should be promoted by the Department of Agriculture—receive the proper honor that is deserved by them for what they do to continue to put food on the table and continue to bring forth the values from those who built this great country.

I thank my friend and colleague, the Senator from Kansas, for bringing this to the attention of the Nation.

Mr. MORAN. Madam President, just to conclude my remarks, I would indicate that my family and I will be eating more beef, not less. I would urge Americans to respond in that way. It is an opportunity for us to support the cattlemen and the livestock producers of our country at a time when they are selling their herds because the drought is so severe that there is no grass and no feed to feed the cattle. As a result, the market is depressed and prices are lower because there are so many sales occurring. We can help our livestock producers, our farm and ranch families in the country, by having a hamburger or steak. Let's go back to that traditional American meal of ''let's eat beef.'' The front of my truck at home says ''Eat Beef,'' and I would encourage Kansans and Americans to do so at this time when our livestock producers, due to the drought, are struggling so greatly.

I yield the floor.

The PRESIDING OFFICER. The Senator from Wyoming.

Mr. BARRASSO. I ask unanimous consent to speak as in morning business.

The PRESIDING OFFICER. Without objection, it is so ordered.

A SECOND OPINION

Mr. BARRASSO. Madam President, I come to the floor today, as I do week after week since the health care law was passed, to give a doctor's second opinion about the health care law that I believe is bad for patients, bad for the providers, the nurses and the doctors who take care of those patients, and terrible for the American taxpayers.

I come to the floor today reminding myself and the Senate of some promises the President made during the health care debate. The President had a couple of key promises. The first was he stated that health insurance premiums would go down. The second promise he made was that if a person likes their insurance plan, they can keep it.

The President actually reiterated the second point after the Supreme Court issued its decision regarding the health care law a few weeks ago. From the East Room of the White House, the President proclaimed:

> If you're one of the 250 million Americans who already have health insurance, you will keep your health insurance.

Perhaps the President does not know that his health care law has already forced many colleges and universities to stop offering their student health plans or perhaps the President is unaware that one can no longer purchase a child-only health insurance policy in many States, including my home State of Wyoming.

Apparently, the President has not spoken to businesses across the country that must actually deal with the ramifications of his health care law. I speak with business owners around Wyoming every weekend as I travel around the State, and the people with whom I speak believe the law will increase the cost of their insurance, increase the cost of their care, and make it more difficult for them to provide insurance for their employees.

Now we have a new study—a report that has come out from the Deloitte consulting firm—and it has spoken to businesses all across the country about the law. The results were compiled in their 2012 survey of employers. In this report, the company did random surveys of 560 companies with 50 or more employees. These results are only from companies that currently offer health insurance to their employees.

So what are the results? Well, the results are not encouraging. They found that approximately 1 in 10 employers is considering dropping the health coverage they currently supply to their employees over the next few years. Specifically, they found that 9 percent of companies expect to drop their insurance coverage, while another 10 percent of respondents said they weren't sure about how they would proceed. The survey revealed that small businesses—those with between 50 and 100 workers—are going to be hit especially hard by this new health care law.

Thirteen percent of the businesses in this category stated they would drop their insurance coverage in the next 1 to 3 years. Thirteen percent of all of those small businesses with between 50 and 100 employees plan to drop their insurance within 1 to 3 years.

Keep in mind that the nonpartisan Congressional Budget Office did some evaluations and thought that only 7 percent of workers would lose their employer-provided health insurance starting in 2014 because the President, looking straight into the camera straight from the White House, said, ''If you like what you have, you can keep it.''

Companies also made it clear that how implementation of the health care law moves forward would impact their

decisions. How so? Here is an example: Approximately one-third of the companies stated they might decide to stop offering health insurance if they find that the law passed by the Democrats in this Senate, along partisan lines—if these companies find that the health insurance under the law and required by the law requires them to offer more generous benefits than they currently provide, they are likely—one-third—to discontinue providing health insurance.

Why is that? Well, it is because the President's health care law actually mandates what kind of insurance companies must give to their employees. This is what is called the essential health benefits package or, as most Americans refer to it, government-approved insurance. It may not be the insurance you want or the insurance you like; it may not be the insurance you need or it may not be the insurance you can afford. No matter how we look at it, the President and those who supported this law say they know better than American consumers, American workers, and people in need of insurance.

So instead of allowing businesses and workers to decide what kind of insurance they need, the health care law empowers Federal bureaucrats to make this decision.

In an article that recently appeared in the Wall Street Journal, the chief financial officer of McDonald's stated that he thought implementing the health care law could cost his company more than $400 million a year. So businesses that decide they can't afford to offer this government-approved insurance are going to be forced to pay a penalty.

How big is the penalty? That is a legitimate question. The Supreme Court says it is a tax—a tax. So they are going to have to pay a tax. So for companies with over 50 employees, they will have to pay, starting at $2,000 per worker. That sounds like a lot of money, but keep this in mind: In 2011 the Kaiser Family Foundation found that the average cost of employer-provided health insurance for families was over $15,000. So they can decide: Do they pay the government $2,000, that tax, or do they pay $15,000 for the insurance? This means many companies would have a sizable financial incentive to simply drop the insurance.

So then what happens? What happens to these folks who previously had the insurance the President said they could keep? Of course, we all know they can't because, once again, the President misled the American people—I believe intentionally. Well, then these employees who were dropped would have to enroll in a government-run exchange. So what happens in the exchange? Well, many of these individuals would qualify for subsidies from the Federal Government to help them purchase insurance—subsidies from the Federal Government to help them pay for insurance that they were previously getting at work, but now because of the health care law they can't get it anymore.

So who is going to end up subsidizing this? The American taxpayers are now going to be paying for the health insurance instead of the employer. This is not only going to cause many Americans to lose their health insurance, but it will also make the $1 trillion health care law even more expensive than the Congressional Budget Office said this past week.

Many businesses surveyed stated they do not intend on dumping the health insurance plans, but they said something else. They said they are not going to stop providing it. Instead, employers are saying to workers: If you want to keep this, you are going to have to pick up the additional cost of your insurance coverage, and you are going to have to do it by helping to pay higher copays, higher deductibles, or participating and contributing to the higher premiums we are going to have to pay.

So for those Americans lucky enough to keep their employer-provided coverage, they will now be paying more money for that privilege. This means employees have essentially two alternatives under this health care law. Either they will lose their employer-provided coverage or they will be facing higher insurance premiums.

For over 150 million Americans who receive their insurance through their employer, neither of these choices is a good one. It didn't have to be this way. That is why I remain committed to repealing the President's health care law and replacing it with patient-centered reforms that will allow patients to get the care they need from a doctor they choose at lower cost.

Thank you, Madam President. I yield the floor.

The PRESIDING OFFICER. The Senator from Minnesota.

Ms. KLOBUCHAR. Madam President, I ask unanimous consent to speak in morning business for up to 15 minutes.

The PRESIDING OFFICER. Without objection, it is so ordered.

Ms. KLOBUCHAR. I am here to talk about two very different subjects, two very different bills. One is the farm bill, and one is the Violence Against Women Act. Both bills are stuck over in the House of Representatives, and both bills should pass. Both bills received significant bipartisan support in the Senate. I am simply asking my colleagues in the other body to get their job done and to get these bills passed.

THE FARM BILL

I will start with the farm bill. Minnesota is fifth in the country for agriculture. It means a lot to our State, it means a lot to the rural areas, but it is also tied to our metropolitan area with our farm businesses, with our food producers, and it is clearly tied in with the rest of the country. This spring's talk of a bin-busting crop has burned away under the extreme summer heat. Farmers and ranchers across the country are experiencing what the U.S. Department of Agriculture is calling the most widespread drought we have seen in decades.

With nearly 90 percent of the corn and soybean crops being grown in areas impacted by the drought, the crop losses are being felt not just by our grain farmers but also are driving up feed prices for our livestock, poultry, and dairy producers. As we well know, dairy producers have already come off some very difficult years.

Higher feed costs for cattle, pork, poultry and dairy impact all Americans at the grocery store. Yesterday the USDA estimated that consumers could expect to pay 3 to 4 percent more for groceries next year at this point.

While some people might think that food magically appears on their tables or in their grocery stores, in Minnesota we know food is produced every day by our farmers. Farmers stand behind each General Mills box of Cheerios or every Jennie-O turkey on the dinner table. That is why when I travel our State I am always reminded of the critical role farming plays in our State's economy and in our country's economy. It has, in fact, been one of the brightest spots. Minnesotans in rural communities and larger cities all benefit from a strong farm economy that provides jobs at farms, mills, processing plants, and equipment manufacturers.

While Congress can't do anything about the lack of rain, we shouldn't make this disaster worse by delaying the passage of the farm bill, which gives farmers and ranchers the assistance they need to help weather this disaster and the certainty they need to make plans for next year and the year after and the year after that. The fact that the 2008 farm bill was a 5-year time period was key to the stability in the rural areas. It was key so farmers could plan ahead. It made a difference during the downturn. We need to do that same thing again.

I think it is a mistake for the House leadership to delay further action on the farm bill. These bills are never easy, but in the Senate we were able to work through 70 amendments before passing the bipartisan farm bill with a strong 64-to-35 vote. Maybe they should do the same.

As part of our responsibility to do more with fewer resources, this bill includes over $23 billion in cuts over the 2008 farm bill. We eliminated direct payments, further focused farm payments on our family farmers, and worked to eliminate fraud and waste through the farm bill to ensure these programs are efficient and targeted.

President Eisenhower was famously quoted as saying this:

> Farming looks mighty easy when your plow is a pencil and you're a thousand miles from the corn field.

I fear that some in Washington have taken that same position and are content with kicking the can down the road and leaving rural America in the lurch. Well, those of us in the Senate

who supported this bill—Democrats and Republicans—were not content with putting our heads in the sand. We weren't content with just letting the crops burn out in the fields. We wanted to get something done.

There are those in the House, such as Representative COLLIN PETERSON of Minnesota, who are trying valiantly to get this farm bill through the House. We must let them do this.

The Senate passed the 5-year farm bill because it is important. It is important because it strengthens the crop insurance program, it funds livestock disaster programs for this year, and continues the program through the end of the farm bill. It ensures that the programs farmers use to get help through tough times, such as the emergency financing credit program or disaster grazing authorities, will be continued with unbroken service.

The farm bill also includes two of my amendments that will help farmers get through these tough times. The first amendment reduces the cost of accessing crop insurance by 10 percent for beginning farmers. This is critical because beginning farmers are less able to afford crop insurance protection and are under greater financial stress because of the drought.

The second amendment eliminates the penalty for beginning farmers that graze livestock on CRP land. This will help beginning ranchers struggling with high feed prices and will also benefit all livestock producers by freeing up the corn to be fed to other animals.

Secretary Vilsack is working at the USDA to help producers with this drought. Under his leadership, the USDA has streamlined the disaster declaration process, reducing the time it takes to start getting help for impacted counties by 40 percent. They reduced the interest rate for emergency loans, as well as reduced the penalty for producers grazing livestock on conservation reserve program acres from 25 down to 10 percent.

While these are important steps, they in no way replace the help farmers in this country will get from this farm bill. We all know it is not just a farm bill, it is a food bill. Only 14 percent of this that we look at is farm programs. The rest are conservation programs. The rest are important school lunch programs. This is a farm bill for the country not just the rural areas. But we can see—anyone who drives through Wisconsin, anyone who drives through Indiana or Missouri or Iowa can see—firsthand why we need this safety net for our farmers, why we need this safety net for our country.

We plead with the House to get this done, to follow the leadership of COLLIN PETERSON and those of us in the Senate who, on a bipartisan basis, got this farm bill done. They need to take it to the floor.

VIOLENCE AGAINST WOMEN ACT

Madam President, as I mentioned, there is a second bill that has also been hung up, a bipartisan bill that received significant support in the Senate—in fact, it got the support of every single woman Senator in this body, Democrat and Republican—and that is the Violence Against Women Act.

Here in the Senate we passed that reauthorization bill in April on a bipartisan 68-to-31 vote. Getting to that point was a tough road. It was not always clear we were going to pass the bill. Just like the two reauthorizations from 2000 and 2006, our bill strengthens current law and provides solutions to problems we have learned more about since the Violence Against Women Act was first passed in 1994. Ever since then, this bill has been able to get through both Houses on a bipartisan basis without significant controversy.

We do not want to go back in time. We do not want to go back to a time when we treated women who were victims of domestic violence like they were not really victims, like it was something they should just expect to happen. We do not want to turn back on the great strides we have made.

One of the improvements in this current bill focuses on a particularly underserved community: women living in tribal areas. We have a number of reservations in Minnesota, and it is a heartbreaking reality that Native American women experience rates of domestic violence and sexual assault that are much higher than the national average.

Our committee, the Judiciary Committee on which I serve, worked closely with the Indian Affairs Committee to come up with some commonsense solutions to the horrific levels of domestic violence and sexual assault in tribal areas.

One of the problems on tribal lands is that currently tribal courts do not have jurisdiction over non-Indian defendants who abuse their Indian spouses on Indian lands, even though more than 50 percent of Native women are married to non-Indians.

The bipartisan Senate bill addresses this problem by allowing tribal courts to prosecute non-Indians in a narrow set of cases that meet three specific criteria: the crime must have occurred in Indian Country; the crime must be a domestic violence offence, and the non-Indian defendant must live or work in Indian Country.

That is the way we get these cases prosecuted. I do not think we believe the Federal courts are going to come in and handle all these domestic violence cases. This is the pragmatic solution that protects these Native American women.

As we were considering the Violence Against Women Act on the Senate floor, many of us had to work very hard to get the message out there that VAWA was and always has been a bipartisan bill—one that law enforcement and State and local governments strongly support.

Throughout this entire process, under the leadership of Senator LEAHY and Republican Senator CRAPO, who did this bill together from the beginning, I have found it very helpful that whenever I needed to tell people why we needed to pass a reauthorization bill, I could point to the great work that my State is doing to combat domestic violence.

There is the legacy of Paul and Sheila Wellstone, who were there at the beginning ushering this bill through in 1994.

Minnesota is the home to many nationally recognized programs.

The Hennepin County Domestic Abuse Service Center that I was honored to be in charge of during my 8 years as county attorney in Hennepin County is a nationally recognized center. We opened one of the first shelters in the country in 1974, and the city of Duluth was the first city to require its police officers to make arrests in domestic violence cases.

I have learned about a unique domestic violence court that Stearns County—that is the area around St. Cloud—has implemented using money from VAWA grants. The partnership, which involves trained people from all levels of the criminal justice system, has allowed 58 percent of the victim participants to separate from their abusers.

Washington County relies on cutting-edge research to provide direction for officers to take appropriate action when responding to domestic violence calls. It is the only program of its kind in the entire country.

These are the kinds of innovative initiatives from law enforcement that are especially critical to combating violence and are directly a result of the Domestic Violence Against Women Act that we have worked so hard to pass in past years in this Congress.

I want to stress just how crucial it is that we get this bill signed into law. We have made a lot of progress over the years, and we have been able to work together across the aisle to build on VAWA's successes. But we should not just send any bill to the President. As you know, the House has passed its own reauthorization of VAWA, which, unfortunately, does not include many of the improvements the Senate bill includes, including the one I mentioned on tribal courts. It also rolls back some of the important improvements that have been made to VAWA in the past.

I am hopeful we will be able to iron out these differences as we move forward, but I strongly believe the improvements that were included in the Senate bill should remain a part of the bill that gets sent to the President. I hope our colleagues in the House will follow suit with the Senate on this domestic violence bill, pass a bipartisan bill, get this done, and get it done soon. It simply is not that hard. Just look into the eyes of a domestic violence victim, look into the eyes of the children, and you know it is not that hard.

I yield the floor.

The PRESIDING OFFICER. The Senator from Arizona.

Mr. KYL. Madam President, I just want to make a very brief comment

primarily for the benefit of our Republican colleagues who have been inquiring about whether we would have, and when we would have, a vote to invoke cloture to proceed to the cybersecurity legislation.

I am hopeful we can do that very soon. From my perspective, it would be wise for us to move forward, to go to the bill, and see if we can work things out. There have been discussions between various groups who are interested in the subject. They are now all talking to each other, which is a very good sign because it is amazing how, when Senators get together and talk to each other, sometimes we can actually accomplish things in a bipartisan way.

So my hope is that we can do that. If it turns out it does not work out, we can always vote no at the end of the day. But I believe we should go forward, that we should get on the bill, and, therefore, I intend to support cloture on the motion to proceed to the cybersecurity legislation.

I thank my colleagues for yielding.

The PRESIDING OFFICER. The Senator from Texas.

Mr. CORNYN. Madam President, I appreciate the courtesy of my colleague from Maryland, and I promise I am going to be just no more than 10 minutes.

TAX HIKES AND SMALL BUSINESS

Two years ago, Members of both parties in this Chamber recognized that America's economic recovery was fragile, too fragile to absorb a tax increase. Since then, obviously, my colleagues across the aisle have changed their minds and experienced a change of heart.

Yesterday the Senate voted to raise taxes. I have been amused by some of the headlines I have read that say the Senate voted to cut taxes, which is false. The Senate did not vote to cut taxes; the Senate voted to maintain the tax rates that have been in existence for 12 years for a certain class of taxpayers, while raising taxes on everyone else.

I cannot explain the logic behind this vote. I can only assume it is some election-year calculus designed to galvanize the political base of our friends across the aisle. It most definitely is not good economics, and it is not good for job creation.

For 3 years, it is no secret America has been living through the weakest economic recovery since the Great Depression. We know from history, from economics, and from common sense that the last thing you want to do amid persistently slow economic growth is to dramatically raise taxes on income and investment. If you want more economic activity, if you want growth, then you do not burden it further. You relieve those burdens, which allows it to flourish and grow, which creates prosperity and jobs. Yet our friends across the aisle just voted to raise taxes on nearly 1 million American businesses.

Many American businesses do not operate as a corporation. They operate as a sole proprietorship, a partnership—in other words, a mom-and-pop operation—or even as a subchapter S or some other legal entity, which causes business income to be paid on individual tax returns not on a separate corporate tax return.

The bottom line is, when we raise taxes on people in the top tax brackets, we inevitably are going to capture, in this instance, 1 million different individuals paying business income on an individual tax return, which is bad for the economy, bad for jobs.

We should make no mistake about it: Given our anemic growth rates, given the ongoing debt crisis in Europe, and given the economic slowdown in China and other emerging market countries, raising taxes on so many job creators could easily tip the U.S. economy back into recession. If we take yesterday's vote to increase taxes on so many small businesses together with the unwillingness to deal with the single largest tax increase in American history—which will occur on December 31, 2012, and is something that has been called taxmageddon, when virtually all the tax provisions in the code will expire, the ones passed 12 years ago—if we combine that huge tax increase with the sequestration, $1.2 trillion, which comes disproportionately out of defense spending, without exception the economists I have talked to say we will be in a recession.

Why is it that our colleagues across the aisle are willing to risk putting America back into recession just to raise taxes? I cannot understand that, unless they have taken some kind of poll, done some sort of focus group that has laid out some strategy which is not readily apparent to most people.

So the idea that this tax increase would solve our fiscal problem is laughable. As my good friend, the Republican leader, said yesterday, the additional revenue generated by the taxes that our Democratic friends voted for yesterday ''[wouldn't] even fund the government for a week.'' A week—and that is before we consider the harmful impact on the economy and jobs.

Whenever I talk to business owners back home in Texas, they express utter bewilderment as to why Members of Congress would want to raise taxes during the current economic environment. Don't our friends across the aisle realize how many small businesses are struggling to stay afloat? Don't they realize that our Byzantine Tax Code and misguided regulations are already strangling job creation? Don't they realize our national unemployment rate has been stuck at more than 8 percent for 41 consecutive months?

No one here wants to see another recession, but apparently some are willing to risk a recession by putting ideology ahead of sound economic policy. After last night's vote, I thought of all the Texas entrepreneurs—more than 400 of them—who have contacted my office, sending their personal, inspiring American success stories. These stories remind us that the American dream is still alive, and it is inextricably intertwined with our free enterprise system. It is not a gift from government. It is what people earn as a result of hard work and the opportunities given to them in this great country.

These stories remind us the American dream is not dependent upon government assistance. It is not about taxing certain people to pay for ideologically driven government projects like Solyndra. It is about offering all Americans the opportunity to earn their success and achieve their dreams.

My office has received literally hundreds of entrepreneurial success stories from Texas, stories such as that of Gary Murray, a Vietnam veteran who came home from the war after three tours as a marine in Vietnam, who spent two decades working at IBM and then launched his own fencing club—a fencing club. For more than a quarter century, Gary's Round Rock Fencing Club has been training young Texans and producing world-class talent, including two Olympians, one world champion, and eight national champions. It is a remarkable story about someone deciding this is what they wanted to do, this is where their passion lies, making the most of it, and creating opportunities for other people.

Gary started the Round Rock Fencing Club with his own money, without any financial support from the government. What he achieved, he achieved on his own. His story is a testament to hard work and human creativity. As Gary puts it: ''The only support I ever got was from my wife and family.''

There are many other business owners like Gary Murray all across Texas and all across this great country.

Before my colleagues advocate higher taxes on these businesses, perhaps they should spend some time talking to the job creators and small business people and the entrepreneurs about the myriad challenges and obstacles government places in their way because of high taxes and overregulation. I suspect my colleagues might learn something.

I yield the floor.

The PRESIDING OFFICER (Mr. SANDERS). The Senator from Maryland.

AFFORDABLE CARE ACT

Mr. CARDIN. Madam President, I have taken the floor before to talk about the health care reform bill, to comment on the Supreme Court decision, which I believe history will show was clearly the right decision. It was the right decision on the law giving the Congress the power to legislate in an area where there is a national need, as the legislature did in the 1930s with Social Security and in the 1960s with Medicare.

The health reform proposals that were adopted by Congress are within the purview of the legislative branch of government. The Supreme Court upheld that right in that decision. I also said it was the right decision because it allows us to move forward on

a path toward universal coverage, where all Americans are guaranteed access to affordable health care. America will now join all of the other industrial nations of the world to say health care is a right, not a privilege.

The legislation that was passed, the health reform bill, has already helped American families. Let me talk about an area—I could talk about many—about what it has done in protecting our consumers against the practices, the arbitrary practices of health insurance companies. We already are seeing that it is in effect where families are being able to take advantage of the fact there are no longer any lifetime caps on health insurance policies. By 2014, we will eliminate annual caps on benefits on health insurance plans. We already have seen for our children the elimination of preexisting conditions, so our children can get policies without having restrictions on what is covered and what is not covered. By 2014 we will see that the preexisting conditions for everyone will no longer be an obstacle to full insurance coverage. That is particularly important for women, where we know at times they have been held to a preexisting condition because of a pregnancy or being the victim of domestic violence.

We have seen discrimination in premiums against women. That no longer will be the case. I could talk about many Marylanders who are happy today because they can stay on their parents' insurance policies—the fact that they are over the age of 21. They can now stay on that policy until age 26.

I want to talk about one other aspect of this law that may not be quite as familiar to our constituents. This provision will take effect on August 1, but we already are seeing the benefits. What I am talking about is the 80–20 rule, where health insurance companies must give value for the premium dollar to the beneficiary. At least 80 percent of the dollars we pay for premiums must go for benefits.

Let me share with you a letter I received from one of my constituents. She wrote:

> I recently had a pleasant surprise. . . . two checks from my health care [insurer] that were rebates on premiums paid. I am someone who has to buy individual health coverage and have been doing so for the last 8 years. The premiums are high and the deductible is high—so I am essentially paying a high price for catastrophic coverage while still paying for individual doctor visits, prescriptions, etc. It is frustrating, but the choices are limited and expensive for individual coverage, and you don't really know how good your coverage is because you don't use it unless you have a major medical event. My premiums go up every year despite the fact that I don't file claims. This month I received a check in the amount of $139 from my current [insurer] and over $300 from a previous [insurer]. Both checks were rebates as a result of the new health care act.
>
> I did not realize it, but the act requires insurance companies to use 80% of the premiums they collect on health care costs. . . . and neither of them hit that percentage and were thus required to provide a refund. Wonderful! The bill is so complicated that I do not understand a great deal of it—but am very pleased with this aspect which seems to go a long way in helping keep health care costs reasonable and prevent consumers from being gouged . . . So thanks to the Senator and all who helped with this health care act.

I bring this to my colleagues' attention, because there are going to be millions of American who are going to be getting rebate checks, and some are going to start scratching their heads, wondering where it is coming from. They are going to be saying: Gee, I guess I made a mistake in the premiums I paid. They are returning them. They are getting those checks because of the passage of the health reform bill, and the provision in the health reform bill that requires insurance companies to give value for the premium dollars we pay.

That protection is now the law of the land. Thanks to the acts of Congress and President Obama, and the Supreme Court upholding the law, those rebates are going to be received. The number of people in the country is 12.8 million Americans who are going to get rebate checks worth about $1.1 billion. Average rebate: $151. That is real money for people who are struggling with their health care needs.

I am proud that in the State of Maryland, there is going to be $27 million made available to 141,000 Marylanders, with an average rebate of $340 for those who get rebates in my State. Let me break this down a little bit further. In the individual market, like the person I received the letter from, the rebates for the people in Maryland will actually average a higher amount. They will average $496. I think that speaks to the fact that insurance companies have hedged their bets in the individual market. They tell us that, you know, we have got to charge a lot more because we do not know what we are getting, when in reality they are making a lot more money in the individual market.

So for the people of Maryland, 38,000 of them are going to get, on average, close to $500 in rebates thanks to the passage of the Affordable Care Act, thanks to the passage of health reform, and thanks to the Supreme Court upholding our right to do it.

The same thing is true in the small group markets where we find that there will be 3.3 million Americans getting rebate checks who are in the small group markets. These are the markets, of course, in which again the options were not as great, more difficult, because of insurance carriers not being as anxious to insure people in small group markets as they are in the larger markets.

The average rebate per family will be $174. In Maryland that number again is higher, $310 for the 13,000 people in Maryland. It also applies to those in the large group markets. These are the large plans. They also are going to see rebates because the insurance carriers charged excessive fees. And they are going to get premium dollar rebates. Some 5.3 million Americans in these large plans will see rebates that average $135. In my State of Maryland, it will be 89,000 people, with rebates averaging $268 a family. These are 1-year numbers. These continue every year. So let me tell the people of Maryland and the people of this country what you can expect. You might get a check that will be delivered to you in the mail. It will be a rebate check. That is as a result of the passage of the health reform bill. You might also see a deposit into the account that automatically pays for your health premiums, because the insurance carrier can make a direct deposit into the accounts which are paying for these premiums.

It is possible you might find a reduction in future premiums. They can use it to reduce your future premiums, but they have to let you know that, so you realize you are getting the rebate, but it is being applied against future premiums. Or if the employer is paying the premiums, the rebates will go to the employer, but the employer must use it to benefit your plan. They cannot use it for themselves. It is used to help again the beneficiary. You will get notice of that.

My purpose again is to make it clear that you would not have gotten these rebates but for the protections that are in the Affordable Care Act. I know my colleague from Vermont and I have been on the floor many times pointing out that all Americans, not just those who do not have insurance today, not just those who might have been discriminated against because of preexisting conditions, not only that 24-year-old who is now on her parent's policy, but all Americans have benefited from the Affordable Care Act, the protections that are in it.

Now millions who thought they were being treated unfairly by their insurance companies are going to be able to get rebates because of excessive premiums. The rule works in combination with another provision of the law that requires rate review to ensure premium increases are reasonable. In other words, we have put into the law protections against unreasonable increases in your premiums. Insurance companies are now required to justify any premium increases of 10 percent or higher. Most States now have the authority to determine whether these increases are excessive, while HHS reviews rates in States that do not operate under effective rate review programs.

That is how federalism should work. States have an opportunity to act. If they do not have adequate review, we have national backup and protection to make sure the rate reviews are being handled in the appropriate way. So as our constituents start to get the benefits—another benefit of the health reform bill, and there are many more that are starting to take effect, and we will hear about some more of those next week, on August 1—I wanted my constituents of Maryland and my

friends around the Nation to know we have provided that you get value for the premium dollar you pay for your health insurance.

We back that up with enforcement, so if there are excessive premiums being charged, the insurance carriers must rebate those premiums to you. Millions of Americans will get the benefit, starting now. We are pleased that this type of protection is in the Affordable Care Act.

I yield the floor and I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The assistant legislative proceeded to call the roll.

Ms. STABENOW. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

THE FARM BILL

Ms. STABENOW. Mr. President, I wish to take a few moments to update folks about what is happening as it relates to the very important effort to pass a 5-year farm bill for our country—for our ranchers, for our farmers, for those who care deeply about nutrition and conservation policy for the country.

We have somewhere between 16 and 20 million people who work in this country because of agriculture—the farm bill and food policy—and I am very proud of all the work we did together to pass a bipartisan farm bill. In doing that, we sent a very strong message on a number of fronts that we were committed to economic certainty for our growers. We said we understand the need to have long-term policies in place, and we also sent a message about disaster assistance.

I have spoken on the floor before, as my colleagues have, about the very serious situation happening all across our country as it relates to livestock and the broad question now of drought in every region of the country. We also have had areas, in addition to drought in Michigan and other places, where food growers have been hit with an early warming and then a freeze again. So we have had multiple reasons to care about short-term disaster assistance, and I am very proud the bill we passed includes a very good livestock disaster assistance program available for this year which will be very helpful for our livestock producers.

We also added provisions for fruit growers that will help those who don't have access to any crop insurance. That will not only include this year, but we looked to the future by putting in new options on crop insurance, new tools for the risk management agency to develop with growers, with commodity groups across the country crop insurance for the future. So as we see these kinds of weather disasters, they will have more certainty because there will be better coverage and broader kinds of coverage for crop insurance for all commodities, which we don't have today.

We definitely need to pass a farm bill. We need the House to pass a farm bill both for long-term policy but also for disaster assistance right now, and we know this is an opportunity to achieve deficit reduction. The only bipartisan effort we have had on deficit reduction on the Senate floor—and I would argue probably bipartisanship on the House floor as well—has been through the farm bill, with $23 billion in deficit reduction, with major reforms, changes in policy, and eliminating four different subsidies that are there when growers don't need them or for things they don't plant anymore and replacing that with a risk-based, market-based system for when farmers truly do need us, as they do now.

So there is a whole range of things we have done—reforms and strengthening conservation efforts in our country, focusing on the right policies around nutrition, around local food systems and so on—and all that is in jeopardy at the moment because the House, rather than bringing to the floor the bill passed out of the House committee, which, even though it is different and I would argue doesn't have all the reforms we have and takes a little different approach on commodities and so on, it is a bill we can work with to come to final agreement on between the House and the Senate. But instead of bringing that to the floor, getting it done, we are now hearing discussions about just passing some kind of a disaster assistance program.

Certainly, we need to do that. We have already passed it and we can strengthen it as we move forward to a conference committee and I would support doing that as well. But instead of having a full 5-year farm bill policy, they are talking about kicking the can down the road one more time. That seems to be a very popular strategy around here. It is not one the public wants us to use. They want to extend the farm bill for another year, with no deficit reduction, no reform, no certainty for farmers, and with policies extended another year that don't work for a lot of industries and then just do some disaster assistance. I think that would be a disaster.

I know we have colleagues on both sides of the aisle—and I am grateful for the leadership of the chairman and ranking member in the House for their advocacy and leadership—who want to get this done, but we need to know the House leadership will allow that to happen so we can get real reform, deficit reduction, and the kinds of policies we need in place that will solve problems and provide the safety net all our farmers need. If we end up in a situation with just an extension, what happens? As our distinguished Presiding Officer knows, it would keep in place for another year a dairy policy that doesn't work.

I remember, in 2009, sitting around the table and talking about what was happening to dairy farmers—folks going out of business, losing their farms because of policies that didn't work. Now the House is talking about extending those policies for another year rather than adopting the changes and the reforms we have put in place that would help dairy farmers all across the country. They are talking about an extension that would eliminate about half the support for fruit and vegetable growers that we put in place. In the last farm bill, I was proud to offer that, and we strengthened that in this farm bill. It is one of the largest areas of commodities, groups of commodities, in the country. So that would not be continued.

There are a number of things that, frankly, would not be continued or available, and there are a number of things that would continue that are bad policy. So if we have a 1-year extension, we are continuing something we rejected and that everybody on both sides of the aisle in the House and Senate said they didn't want to do, which is direct payments going to farmers, government payments, regardless of whether the prices are high or low, in good times or bad times, and continuing even on things that aren't grown anymore. We all said that makes no sense.

We all said, instead, that we wanted to move to a risk-based system and have a strong safety net there when farmers and ranchers need us, to strengthen crop insurance and make sure farmers have skin in the game; that they are sharing in the cost on crop insurance.

But none of that happens with a simple 1-year extension. We continue things we have all said are not good policy, that cost taxpayers money, and that we shouldn't be spending our money on at a time of huge deficits; that we should not have those kinds of subsidies in place. We eliminated four of those, with $15 billion in savings alone in the commodity title. All that would go away under what the House is talking about. We would be continuing things people have said were bad policy. Everyone talks about reforms and changes, but this would continue the old ways.

We eliminated about 100 different programs, duplication, and things that do not work anymore—redundancy, whatever it is. About 100 different programs we eliminated in what we passed. They would all continue—every single one of them—for another year if we just do a 1-year extension.

Let me just say in conclusion that I encourage House colleagues to join with us. We can have differences in what our commodity title looks like, and I respect those differences. We can work those out if we have the opportunity to negotiate in good faith and get things done. We will do that. We can have differences in what should happen in the nutrition title, but we should not be saying to farmers and growers that we are going to walk away from them and put in place another kick-the-can-down-the-road

strategy that keeps bad policy or no policy going, no deficit reduction, and puts us in a situation where, frankly, 1 year from now it is tougher and it is a bigger mess than ever, with our growers trying to go to the bank, trying to figure out what they are going to do when planting season comes and making decisions, all the while looking at us and asking: What happened here? Why did you do this?

We did our job in the Senate on a strong bipartisan basis. It was a lot of hard work. We spent a lot of time here. We need to complete the job. If our House colleagues will come together with us; if the Speaker, the leadership in the House, will decide to give us a vehicle with which to do that, I am very confident we can get the job done.

I yield the floor.

The PRESIDING OFFICER. The Senator from Connecticut.

Mr. LIEBERMAN. Mr. President, for the information of my colleagues, I know the Senate majority leader is in discussions with the Republican leader, and I know the hope is we can soon have the vote on a motion to proceed to S. 3414. But as yet I have not been informed there has been the necessary meeting of minds. I hope it will be soon, and I hope everyone will support it.

I yield the floor, and I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

Mr. HOEVEN. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

(The remarks of Mr. HOEVEN pertaining to the introduction of S. 3445 are located in today's RECORD under ''Statements on Introduced Bills and Joint Resolutions.'')

Mr. HOEVEN. I suggest the absence of a quorum.

The PRESIDING OFFICER (Mrs. SHAHEEN). The clerk will call the roll.

The legislative clerk proceeded to call the roll.

The PRESIDING OFFICER. The Senator from Vermont.

Mr. SANDERS. Madam President, I ask unanimous consent that the call of the quorum be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

THE ECONOMY

Mr. SANDERS. Madam President, there has been a lot of talk about one of the major issues we as a nation are going to have to deal with, and certainly the Presidential candidates will be talking about it during the next few months, and that is that we have a $16 trillion national debt and we have a $1 trillion deficit. I think all Americans understand this is a very important issue, and it is something we as a nation are going to have to grapple with.

How we deal with the deficit and the national debt is certainly one of the most important and interesting issues we are going to have to address.

What I find interesting is that when we talk about the deficit and the national debt, there seems to be, among some of my colleagues, collective amnesia. It is as if this debt and deficit popped up yesterday and we have no understanding of how we got to where we are today.

I would like to take a moment to remind some of my friends that back in January of 2001—not so many years ago—when President Bill Clinton left office, this country was not running a deficit, it was running a very significant surplus of some $236 billion. That is a very significant surplus. As a matter of fact, in 2001 the Congressional Budget Office projected that we would have Federal budget surpluses totaling $5.6 trillion from 2002 to 2011. In other words, when Clinton left office there was a very significant surplus, and the projection was that surplus was going to go up and up. What happened? Well, that is a question we need a little bit of time to discuss.

I find it interesting that there is no context for deficit reduction. Let me suggest that, in fact, some of the people who come down to this floor and talk the loudest about the deficit and the national debt are precisely those same people who caused the national debt of $16 trillion and a deficit of over $1 trillion.

How did we get to where we are today from the time when Clinton left office and we had a significant surplus? No. 1, many of our deficit hawks who are coming down to the Senate floor telling us about all the programs we have to cut for the middle class, working families, our children, and the elderly, are real deficit hawks. My goodness. When it came to the war in Iraq, many of us voted against it since it didn't make a whole lot of sense. We also noted that our deficit hawk friends went to war—I believe for the first time in the history of America—and forgot they would have to pay for that war. I think some of us might hold a little bit of doubt in some of the comments of our friends about their real sincerity and concern about deficit reduction when they went to a war in Iraq which will end up—after we take care of the last veteran wounded in that war 80 years from now or whenever—costing probably $3 trillion.

Well, if you spend $3 trillion to go to war, forget to pay for it, and then come to the Senate floor and tell us how concerned you are about the deficit and the national debt, some of us are saying: Well, maybe that is not the case. Where were their concerns about the deficit when they went to war when we had a deficit hawk President named George W. Bush? So that is one of the major reasons we are running a $1 trillion deficit right now.

The second reason is—and you don't have to have a Ph.D. in economics to understand it—that if in the middle of a war they decide to give huge tax breaks, including $1 trillion over a 10-year period to the top 2 percent, the billionaires and millionaires, so $1 trillion is not coming into the Federal Government, that adds to the deficit. I ask my Republican friends where was their concern about the deficit and the national debt when they gave $1 trillion in tax breaks to millionaires and billionaires?

The third point I wish to make is that we are in the middle of a horrendous recession. Unemployment is sky high and underemployment is sky high. People have lost homes and their life savings. People are hurting. This recession was caused by the efforts—and I must confess, not just a Republican effort but also a Democratic effort—and the bipartisan desire to deregulate Wall Street because people believed that if we deregulate Wall Street and allow insurance companies to merge with commercial banks and investor banks and we do away with Glass-Steagall, my goodness, those folks on Wall Street—honest people with great integrity—would just create wealth for all Americans. That is what Alan Greenspan, Robert Rubin, and all these guys were telling us. I was a member of the Financial Services Committee in the House and never believed that for one moment. It never made an iota of sense to me. Anyway, these guys fought for deregulation. We had deregulation, and as a result of the greed, recklessness, and illegal behavior on Wall Street, we were plunged into the terrible recession we are in now.

One of the points that are very rarely made on the Senate floor is that today, at 15.2 percent as a percentage of GDP, revenue is the lowest in more than 60 years. So it is easy for people to come to the Senate floor and say we have to cut, cut, cut. They forget to tell us that as a result of the Wall Street-caused recession, at 15.2 percent, revenue is the lowest as a percentage of GDP in more than 60 years. That is an issue we have to deal with.

You know what, we don't increase our revenue when we give more tax breaks to billionaires. We don't increase our revenue when we say that at a time when we have tripled military spending since 1997, maybe we need even more for the military. That is not a way to reduce the deficit.

Now, what do my Republican friends and some Democrats say? Well, they come to the Senate floor and suddenly—after going to war without paying for it, after giving huge tax breaks to the rich, after deregulating Wall Street—realize we have a deficit problem, and they are very concerned about this deficit problem. They come to the Senate floor and say: The only way we can go forward is to cut Social Security. Social Security is funded independently. It hasn't added one nickel to the deficit, but we are going to cut Social Security anyway. We are going to cut Medicare, we are going to cut Medicaid, we are going to cut Pell grants, we are going to cut education,

and we are going to cut environmental protection. That is deficit reduction.

Are we going to ask millionaires and billionaires, who are doing phenomenally well, whose effective tax rate is the lowest in decades, to pay one nickel more in taxes? No, we can't do that, but we can cut Social Security, Medicare, Medicaid, education, and every program that the children, seniors, and working families of this country depend upon.

Now, to add insult to injury in terms of this movement supported by big-money interests that have so much influence over what goes on here in Congress, it is important to look at the playing field of the American economy today to understand what is going on. Are the people on top really hurting and suffering? Are large corporations today really struggling under onerous corporate taxes? The answer is, obviously not.

We don't talk about it enough, and too few people even mention it, but I do, and I will continue. It is important today to understand that the United States has the most unequal distribution of wealth and income since the 1920s and the most unequal distribution of wealth and income of any major country on Earth. Why is that important? It is important to know that. Before we cut Social Security, Medicare, Medicaid, education, and the ability of working-class kids to go to college, we have to know the condition of how people are doing today. The middle class today is shrinking and poverty is increasing. When we cut food stamps and Medicaid, we are going to hurt a whole lot of people, and in some cases very tragically.

Just last week a member of my staff went to southwest Virginia, and she spent the day at a program in which thousands of people in that area were lining up to get dental and health care because they didn't have any health insurance. There are 45,000 Americans who will die this year because they don't have health insurance and can't get to a doctor in time. There are people who say: Let's cut Medicaid. There are people all over this country who can't find a dentist. There are children who are suffering from dental decay. Let's cut Medicaid. Well, I don't think so.

If we look at the country, the middle class is shrinking, people are hurting, but people on top are doing phenomenally well. Very few people talk about it. I am going to talk about it. In the last study we have seen in terms of income distribution in this country—and that is what happened between 2009 between and 2010—93 percent of all new income created over that year went to the top 1 percent. I will say it again. Ninety-three percent of all new income in that year went to the top 1 percent. The bottom 99 percent had the privilege of sharing the remaining 7 percent. Yet, when we ask the people on top to maybe pay a little bit more in taxes, oh my goodness, there are lobbyists all over Capitol Hill saying: We can't afford to. We are down to our last $50 billion. We just can't afford another nickel in taxes. We need that money now. Thanks to Citizens United, we can pump that money into political campaigns.

One family who is worth $50 billion is going to put $400 million into the campaign. Another guy who is worth $20 billion can't pay more in taxes, but he does have hundreds of millions to pour into political campaigns.

In terms of distribution of wealth, which is a different category of costs than distribution of income, we have an incredible situation. I hope people understand what is going on in this country, where one family—one family, the Walton family, of Wal-Mart—now owns more wealth at $89 billion than the bottom 40 percent of the American people. One family owns more wealth than the bottom 40 percent. Do we know what some folks want to do here? They want to repeal the entire estate tax and give that family a very substantial tax break, because owning $89 billion is obviously not enough. They are struggling. We have to give them a tax break while we cut Social Security, Medicare, and Medicaid. If that makes any sense to the American people, I would be very surprised, and it does not make sense to the American people.

According to a February 2011 Washington Post poll, while more than 70 percent of Americans oppose cutting Social Security and Medicare, 81 percent supported a surtax on millionaires to reduce the deficit. My guess is if we go to New Hampshire, Maine, or any other State in America and we say to people, we have a deficit problem and the choice is between cutting Social Security or asking millionaires and billionaires to pay more in taxes, there is, in my view, no State in America—no State in this country, no matter how red it may be—where people will say: Cut Social Security and Medicare and Medicaid, but don't raise taxes on millionaires and billionaires. I don't believe that is true anyplace in America.

Today, the top 1 percent owns 40 percent of the wealth of our Nation while the bottom 60 percent owns less than 2 percent. The top 1 percent owns 40 percent; the bottom 60 percent owns less than 2 percent, and there are Members of this Senate coming to the floor and saying we are going to punish the bottom 60 percent and we are going to give more to the people on top.

There was a study that recently came out that talks about the ability of billionaires and corporations to use tax havens. What we know—and I am a member of the Budget Committee—is that millionaires and billionaires and corporations in this country are avoiding paying about $100 billion every single year by using tax havens in the Cayman Islands, in Bermuda, Panama, and other countries. Maybe, just maybe, before we cut Social Security and Medicare, we might want to pass legislation to make those people start paying their fair share in taxes and do away with those tax havens.

Let me conclude by saying we are in a pivotal moment in American history. If we as a Nation do not get our act together, in my view, we will move even more rapidly in the direction of an oligarchy, where we will have a few people on the top with incredible wealth controlling not only our economy but also, through Citizens United, the political life of this country. We are seeing that playing out right here on the floor of the Senate, with people who are turning their backs on working families and the middle class, and at a time when the wealthiest people are doing phenomenally well, fighting for more tax breaks for people who absolutely don't need them.

I hope the American people pay rapt attention to this debate, and I hope the American people get involved in this debate, because if they do not, mark my words, within 4 months, a handful of people, supported by corporate America and the big money interests, are going to bring down to this floor a deficit reduction proposal which will cut Social Security, Medicare, Medicaid, and give more tax breaks to the wealthiest people in this country. It will have virtually all Republican support. It will have some Democratic support. If we don't aggressively oppose this approach, that is exactly what will happen.

I yield the floor.

The PRESIDING OFFICER. The majority leader.

Mr. REID. Madam President, I appreciate my friend yielding, my dear friend from Vermont.

EXECUTIVE SESSION

NOMINATION OF ROBERT E. BACHARACH TO BE UNITED STATES CIRCUIT JUDGE FOR THE TENTH CIRCUIT

Mr. REID. I ask unanimous consent that the Senate proceed to executive session to consider Calendar No. 759, the nomination of Robert E. Bacharach, of Oklahoma.

The PRESIDING OFFICER. Without objection, it is so ordered.

The clerk will report the nomination.

The assistant bill clerk read the nomination of Robert E. Bacharach, of Oklahoma, to be United States Circuit Judge for the Tenth Circuit.

CLOTURE MOTION

Mr. REID. Madam President, I send a cloture motion to the desk with respect to this nomination.

The PRESIDING OFFICER. The cloture motion having been presented under rule XXII, the Chair directs the clerk to read the motion.

The assistant bill clerk read as follows:

CLOTURE MOTION

We, the undersigned Senators, in accordance with the provisions of rule XXII of the

Standing Rules of the Senate, hereby move to bring to a close debate on the nomination of Robert E. Bacharach, of Oklahoma, to be United States Circuit Judge for the 10th Circuit.

Harry Reid, Patrick J. Leahy, Thomas R. Carper, Tom Udall, Robert Menendez, Kirsten E. Gillibrand, Dianne Feinstein, Kent Conrad, Christopher A. Coons, Herb Kohl, Amy Klobuchar, Jack Reed, Ron Wyden, Richard J. Durbin, Jeff Merkley, Richard Blumenthal, Sherrod Brown.

Mr. REID. I ask unanimous consent that the mandatory quorum under rule XXII be waived.

The PRESIDING OFFICER. Without objection, it is so ordered.

LEGISLATIVE SESSION

Mr. REID. I ask unanimous consent that the Senate resume legislative session.

The PRESIDING OFFICER. Without objection, it is so ordered.

CYBERSECURITY ACT OF 2012—MOTION TO PROCEED—Continued

Mr. REID. I ask unanimous consent that at 3:30 p.m. today, the Senate proceed to vote on the motion to proceed—or what we can do, we will start the vote at 3:25; and if somebody is going to be a bit late, we will protect them on that.

So I ask unanimous consent we start voting at 3:25 p.m. today on the motion to proceed to S. 3414, the cybersecurity bill.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. REID. Madam President, I meant that request to be 3:22 p.m.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. REID. All for my friend from Louisiana.

CLOTURE MOTION

The PRESIDING OFFICER. Pursuant to rule XXII, the Chair lays before the Senate the pending cloture motion, which the clerk will state.

The assistant bill clerk read as follows:

CLOTURE MOTION

We, the undersigned Senators, in accordance with the provisions of Rule XXII of the Standing Rules of the Senate, hereby move to bring to a close debate on the motion to proceed to calendar No. 470, S. 3414, a bill to enhance the security and resiliency of the cyber and communications infrastructure of the United States.

Harry Reid, Joseph I. Lieberman, John D. Rockefeller IV, Dianne Feinstein, Sheldon Whitehouse, Barbara A. Mikulski, Barbara Boxer, Jeff Bingaman, Patty Murray, Max Baucus, Charles E. Schumer, Bill Nelson, Christopher A. Coons, Tom Udall, Carl Levin, Mark R. Warner, Ben Nelson.

The PRESIDING OFFICER. By unanimous consent, the mandatory quorum call has been waived.

The question is, Is it the sense of the Senate that debate on the motion to proceed to S. 3414, a bill to enhance the security and resiliency of the cyber and communications infrastructure in the United States, shall be brought to a close?

The yeas and nays are mandatory under the rule.

The clerk will call the roll.

The assistant legislative clerk called the roll.

Mr. DURBIN. I announce that the Senator from North Dakota (Mr. CONRAD) is necessarily absent.

Mr. KYL. The following Senators are necessarily absent: the Senator from South Carolina (Mr. DEMINT), the Senator from Oklahoma (Mr. INHOFE), the Senator from Illinois (Mr. KIRK), and the Senator from Utah (Mr. LEE).

Further, if present and voting, the Senator from South Carolina (Mr. DEMINT) would have voted ''nay.''

The PRESIDING OFFICER. Are there any other Senators in the Chamber desiring to vote?

The yeas and nays resulted—yeas 84, nays 11, as follows:

[Rollcall Vote No. 185 Leg.]

YEAS—84

Akaka	Franken	Mikulski
Alexander	Gillibrand	Murkowski
Ayotte	Graham	Murray
Begich	Grassley	Nelson (NE)
Bennet	Hagan	Nelson (FL)
Bingaman	Harkin	Portman
Blumenthal	Hatch	Pryor
Blunt	Hoeven	Reed
Boozman	Hutchison	Reid
Boxer	Inouye	Risch
Brown (MA)	Isakson	Rockefeller
Brown (OH)	Johnson (SD)	Sanders
Burr	Kerry	Schumer
Cantwell	Klobuchar	Sessions
Cardin	Kohl	Shaheen
Carper	Kyl	Shelby
Casey	Landrieu	Snowe
Chambliss	Lautenberg	Stabenow
Coats	Leahy	Thune
Coburn	Levin	Toomey
Cochran	Lieberman	Udall (CO)
Collins	Lugar	Udall (NM)
Coons	Manchin	Vitter
Corker	McCain	Warner
Cornyn	McCaskill	Webb
Crapo	McConnell	Whitehouse
Durbin	Menendez	Wicker
Feinstein	Merkley	Wyden

NAYS—11

Barrasso	Johanns	Roberts
Baucus	Johnson (WI)	Rubio
Enzi	Moran	Tester
Heller	Paul	

NOT VOTING—5

Conrad	Inhofe	Lee
DeMint	Kirk	

The PRESIDING OFFICER. On this vote, the yeas are 84, the nays are 11. Three-fifths of the Senators duly chosen and sworn having voted in the affirmative, the motion is agreed to.

The PRESIDING OFFICER. The Senator from Connecticut.

Mr. LIEBERMAN. I will yield to the leader. I thank him, too, for that resounding vote, which seems to me not that the debate is over but the debate is going to begin, and an overwhelming majority of the Members of the Senate want to adopt cybersecurity legislation.

Mrs. MCCASKILL. Mr. President, I come to the floor today to express my concerns about S.3414, the Cybersecurity Act of 2012. Like many of my colleagues, I voted today to allow the Senate to fully debate and consider amendments to this bill, but I want to make it clear that I have some significant concerns about this legislation and unless improvements are made, I cannot support the legislation in its current form.

At the outset, let me just say, I do firmly believe that the Congress should take action to address our Nation's vulnerability to cyber threats. A cyber attack on our critical infrastructure, whether it be our energy grid, a regional water supply, or our financial markets, could significantly harm our economy, our national security, and our way of life. However, the legislation before us today still needs significant improvement before it can become the law of the land.

I have heard from many in Missouri, including many companies operating or associated with the types of critical infrastructure that will be subject to the provisions of this legislation. They have raised concerns that, as currently structured, S. 3414 would create redundant oversight structures and add additional standards. Moreover, the bill may have the effect of creating a new Federal system that these entities will have to comply with even though many already work within well-established systems related to developing security standards and responding to cyber threats. I cannot support legislation that creates new and duplicative systems that will impact Missouri businesses in a negative way. While addressing the critical national security aspects of improving our Nation's defenses against and ability to respond to cyber attacks, cybersecurity legislation must improve the regulatory scheme and streamline processes for businesses, not the opposite.

Additionally, the carrot-and-stick approach that is created by the current bill would limit the sharing of cyber threat information, in a protected fashion, to those private entities which are participating in the voluntary cybersecurity program the bill would create. Those in the program would have to adopt specific standards and in return would receive relevant real-time cyber threat information. Those not accepting those standards and entering the program would not receive the protections of the program and would be limited in the cyber threat information they receive. Given that sharing such information could potentially thwart a cyber attack, it seems absurd that such information would go unshared because a particular entity was not a participant in the voluntary system. Such a provision inhibits the very type of information sharing we are trying to promote in order to enhance cyber security. In this respect, the carrot-and-stick approach simply does not make sense.

I also remain concerned with the scope of responsibility this legislation provides to the Department of Homeland Security. As we have found throughout the history of DHS, it has

relied heavily upon a contract workforce in order to satisfy its mission. At this time, the Department does not have the necessary expertise it will need to guide a multi-agency, multi-sector council in evaluating whether or not proposed cybersecurity standards are sufficient to address the evolving nature of cyber threats. The decision to place DHS in such a critical role leadership role in regards to many aspects of the cybersecurity scheme proposed by this legislation needs to be revisited.

I have other concerns with this legislation, but these are my chief concerns. I am pleased that both of the Senate's leaders have indicated that this legislation will be subject to a robust amendment process. I look forward to evaluating the amendments brought forward to this legislation, and I am hopeful that the amendments will improve the bill enough so that I can support it. If not, I will oppose the legislation and send it back to the committee process, where more work can be undertaken to generate an acceptable piece of cybersecurity legislation. Whether now or in the future, the Senate does need to pass legislation. But it must be legislation that is well crafted, balanced, and workable for the businesses that will operate under its scheme.

I yield the floor.

The PRESIDING OFFICER. The Republican leader.

UNANIMOUS CONSENT REQUEST—H.R. 9

Mr. MCCONNELL. Madam President, shortly I am going to be asking unanimous consent to pass the annual Burma sanctions bill that we have renewed about this time every year for the last decade. The bill was reported out of the Finance Committee on a voice vote last week along with a package of other unrelated measures as part of S. 3326.

Some of my colleagues have some concerns about those other sections. This is unrelated to the Burmese Freedom and Democracy Act. As I indicated, on behalf of my colleagues I have offered—in fact, what I have done in discussions off the floor is offer to find a time to set up a vote on S. 3326 on behalf of my colleagues.

I believe a vote is the best way to resolve the impasse surrounding this bill. However, our friends on the other side have as yet not agreed to that. So in the absence of a vote on the larger bill, I think the best way to proceed is for the Senate to go ahead and pass this important and noncontroversial foreign policy measure today.

This is a very timely issue. These sanctions actually expire today. If we do not act now to extend them, I do not know when the Senate will have a chance to address this important issue. Consideration of this year's Burmese Freedom and Democracy Act comes amidst historic changes that are occurring on the ground in Burma. Aung San Suu Kyi, long a political prisoner of the country, is now actually a member of the Parliament.

The National League for Democracy, once a completely banned organization, now actively participates in political life in Burma. For these reasons and others, the administration, which I support, has taken a number of actions to acknowledge the impressive reforms that President Thein Sein and his government have instituted thus far. The United States has responded by sending an ambassador to Burma. That is the first time we have had an ambassador there in two decades.

The administration also largely waived the investment ban and financial restrictions permitting U.S. businesses to begin investing in that country. However, significant challenges in Burma still lie ahead. Ongoing violence in the Kachin State and the sectarian tensions in the Arakan State reflect a long-term challenge confronting the country related to national reconciliation.

Hundreds of political prisoners remain behind bars. The constitution still has a number of totally undemocratic elements. And the regime's relationship with North Korea, especially when it comes to arms sales with Pyongyang, remains an issue of grave concern to us.

Sanctions with respect to Burma should be renewed in order to provide the administration with the flexibility it needs to encourage continued reforms in that country, to encourage the government to tackle these remaining tough issues. Failure to renew the sanctions could undermine the administration's diplomatic efforts in Burma, which I support, and could send the wrong signal to the Burmese Government that they have done all they need to do. But where are we?

Therefore, the only way I see getting this resolved in time to keep the sanctions from expiring today is for the Senate to go ahead and pass this, and ask the House to pick it up and pass it as soon as they return next week. Hopefully, we can resolve this extremely important issue that other Members have with other sections of S. 3326, completely unrelated to the effort to renew Burma sanctions, and pass those other important trade priorities next week.

In the meantime, this is a terrible message for us to be sending. This is an extremely big issue. It may sound like a small issue; it is a big issue in Burma. Secretary Clinton has been there, I have been there, Senator MCCAIN has been there, and Senator COLLINS. Senator FEINSTEIN has been active on this issue. This is no small matter in a country that we have been hoping would move in the direction of reform, and finally is.

I know there is always a debate about whether sanctions have made a difference. When I was in Burma in January, in addition to meeting with Suu Kyi I was also meeting with government officials. Every single one of the government officials brought up the sanctions. It convinced me that they must have made a difference. Now, because of the changes that have occurred, the administration and I, who have been involved in this issue for two decades, are in total agreement about the way to handle it, which is to renew the sanctions after which the administration will waive a substantial number of them as a further indication that the sanctions remain there, although not currently operative, because of the changes that have occurred in the country. So I think it is a big mistake to have this important foreign policy matter attached to and stymied by, apparently, differences over other unrelated parts of the measure.

Therefore, I ask unanimous consent that the Finance Committee be discharged from further consideration of H.R. 9; provided further that the Senate proceed to its immediate consideration; all after the enacting clause be stricken and the text of section 3 of H.R. 3326 be inserted in lieu thereof.

For the information of Senators, as I indicated, the Burma sanctions language expires today. This would avoid that.

So I finally ask unanimous consent that the bill be read a third time, passed, and the motion to reconsider be laid upon the table.

The PRESIDING OFFICER (Mr. BLUMENTHAL). The Senator from Montana.

Mr. BAUCUS. Mr. President, reserving the right to object, I very much appreciate and admire the efforts of the Senator from Kentucky to keep proposing sanctions on Burma. In fact, the Senator will remember that 3 or 4 months ago I went out of my way to praise the Senator when he stood up for Burma. In fact, he may remember his press office called my office to say thank you. Gosh, Senator BAUCUS thanked the leader, and I meant it. I very much admire the effort and the way the Senator has undertaken to maintain these sanctions.

We are all very proud of Aung San Suu Kyi for winning the Nobel Prize, in London, when she visited Europe not long ago. I remember watching her on television. She has done so much for her country and stood so much for the people of Burma. It is astounding. I have not had the privilege of meeting her personally, but I have watched her from afar and with great admiration and not only would thank her but again thank the Senator for his efforts.

One can say the other matters are unrelated, but one could also say the Burma issue is riding along with the AGOA bill. There are thousands of African women who have lost their jobs because we have not acted on the AGOA bill, and they tend to be single moms—thousands—because they can't get orders to sell in the United States. Consequently, jobs in the United States now are in jeopardy because the AGOA bill has not been extended.

It is true the AGOA bill does not expire until the end of September. That

is true. However, as a practical matter, these women have lost their jobs already because American companies are not taking orders from African countries that are providing the apparel that are otherwise provided for under the AGOA bill. It is a huge issue for those African women who have lost their jobs as well as a lot of American companies that are in jeopardy because they can't receive the apparel from the African companies if this is not extended.

I might say, too, the DR–CAFTA bill is similar. That puts in jeopardy a lot of jobs in South Carolina and North Carolina. So in a certain sense it is a jobs bill. Both these bills are important. They are very important. This package was put together and agreed to by Senators on the committee, Republicans and Democrats both. It was agreed to by leadership offices, both sides. We worked hard, as the leader often does, to get consensus around here. So this was the thought, to put the bills together, and all Republicans agreed.

There was one Senator who said he had a problem with one of the pay-fors, and, frankly, it is a pay-for this body has adopted many times. That Senator himself has voted for this pay-for many times. It just seems to me, if we break up the package, then the package is broken and it puts in jeopardy those other provisions because Senators will want to offer amendments. The Senator from Kentucky well knows, once we start going down that road, things get hung up around here; the main point being these are both very important bills, and the other main point being it was agreed to. This package was agreed to all the way around, and I think at this point it does not make sense to break it up.

So I object.

The PRESIDING OFFICER. The Republican leader.

Mr. MCCONNELL. Mr. President, if I may, I believe the Burma sanctions bill has been renewed without additional matters attached to it for some 10 years now on an annual basis. I am perplexed as to why this year it was turned into a package.

I agree with the distinguished chairman of the Finance Committee that it was agreed to. But there is a dispute between the chairman of the Finance Committee and another member of the Finance Committee who is on the floor, and Senator COBURN can speak for himself. I might say, I don't have a dog in that fight. As far as I am concerned, that is another matter. No matter how important that may be, I doubt a failure to pass the other measure, which doesn't expire until September, creates a major potential foreign policy problem which could well be created by the Burma sanctions bill expiring later today.

I will not argue the rest of the bill is important or unimportant. I frankly don't know much about the rest of the bill. I do know something about the Burma sanctions bill, having offered the original bill 10 years ago and having been on the floor as we renewed it annually during that period, and I am pretty confident this will be perceived in Burma as a problem. It seems to me it is a completely avoidable problem.

As to the rest of it, the Senator from Oklahoma is here and he can speak for himself, so I defer to him and to the chairman of the Finance Committee to discuss the balance of the bill. But it would have been my hope, had the chairman of the Finance Committee not objected, since it was cleared on my side—and it was cleared on my side, regardless of previous understandings about putting the package together, by the ranking member of the Finance Committee, Senator HATCH, and by Senator COBURN—to split the Burma sanctions bill off and pass it freestanding today on a voice vote.

So with respect to the consent agreement I offered, which was objected to, I want to make sure everybody understands there were no objections to it on the Republican side of the aisle.

The PRESIDING OFFICER. Objection is heard to the request of the Republican leader.

The Senator from Montana.

Mr. BAUCUS. Mr. President, I do not want to belabor the point. The Obama administration is opposed to splitting the package apart. They are in favor of keeping the package as it is, and I think for good reason because the administration favors both Burma as well as AGOA and DR–CAFTA. That is the reason. They are both very important. It is for that reason I think it makes sense.

The Senator is correct. It is very easy to resolve this thing by proceeding with Burma and AGOA. But if the leader wants to keep talking, I am more than willing, over the next week, to see if there is another resolution to work this out.

The PRESIDING OFFICER. The Republican leader.

Mr. MCCONNELL. Mr. President, I would just ask a question of the Senator. What I hear is that the Democratic administration and Democratic Senators are opposed to passing the Burma sanctions bill today freestanding? Is that what I hear the chairman of the Finance Committee saying?

Mr. BAUCUS. That is not what the Senator heard me say.

Mr. MCCONNELL. Then why did the Senator object to the request?

Mr. BAUCUS. Because the administration and I want them both.

Mr. MCCONNELL. But the Senator can't get them both unless he can work this out with my good friend, the Senator from Oklahoma, who is on the floor and who may want to address this matter.

Mr. BAUCUS. I am more than willing to sit down and try to work this out, but at this point I think any attempt to split them out is to jeopardize the AGOA bill, and as I mentioned earlier, there are already thousands of women who have lost their jobs in Africa because of our delay in passing AGOA.

The PRESIDING OFFICER. The Republican leader.

Mr. MCCONNELL. Let me make sure I understand where we are. The consent agreement to pass the Burma sanctions bill today, before it expires, is clear on this side of the aisle—clear. The chairman of the Finance Committee has announced, to my surprise, that the administration does not favor allowing Burma sanctions to pass today because it is attached to something related to other matters.

So make no mistake about it, we have, for the first time in the history of this issue, turned it into a partisan matter. We have spoken with one voice in America relating to Burma, under administrations of both parties and Senates of both parties. Yet today, for the first time, we have a partisan split over an issue about which America ought to be speaking with one voice.

I basically have said all I have to say. I do want to hear from Senator COBURN. I know he has strong feelings about the other part of the measure about which I am basically not familiar.

The PRESIDING OFFICER. The Senator from Oklahoma.

Mr. COBURN. Mr. President, first of all, I would like to say I support all three of these measures, in terms of their passing. What I don't support is continuing the habit that has put this country $16 trillion in debt.

To clarify, as a member of the Finance Committee, if one reads my opening statement at that hearing, in that markup, I objected to this bill on the basis of pay-fors. I offered two separate amendments that, on the floor, everybody would agree are germane because the money to pay for the $200 million comes out of trade areas. Yet they were rejected as nongermane by the chairman. So they weren't offered because he said he would reject them. So to create the impression there was no objection to the pay-for in this bill and that everybody agreed is inaccurate, to say the least.

I called Senator COONS of Delaware, who is interested in this, and I called Senator BAUCUS when this came up, and I told him I have a plan so we can get this all done this week. I was willing to lose a vote on the amendment to have an opportunity to offer the amendment and give my side of the story by splitting these two so the House could pass it. The House has now gone home. Burma sanctions are no longer available to be passed, except if we were to do something extraordinary with the House, which I understand from the Speaker can happen. So Burma sanctions could happen this week.

But I wish to go back to the more important point. Regardless of whether I voted for something in the past, using the type of pay-for that is in this bill is what I call the Wimpy mechanism: Wimpy drives up to Wendy's and orders

a hamburger, and when he gets around to the window he says: Don't worry about it, I will be back in 10 days to pay for it. What we have done is use custom user fees over 10 years to collect enough money to pay for $200 million.

With the waste that is in this government, for us to use a 10-year pay-for on something that will be expended over 3 years means we are not capable of addressing the much bigger issues in front of our country. If we can't find $200 million in a $3.6 trillion budget, we are unqualified to be here.

What I would say to my friends and my colleague on the Senate Finance Committee is that somebody has to start saying no. I would remind everyone of a lecture I got from Senator Pete Domenici on a land bill about 2 years ago. He said: We have always done it that way. I said: You know what, you are right, and that is why we are in trouble. So the financing mechanism on this bill denies the situation we are in and charges out over 10 years custom user fees to pay for it.

No other American business, no other company, no other family gets that kind of luxury, especially when they are in debt at 105 percent of their GDP. If we look at where we are, the average American, what we can say is that we are taking in $53,000, we are spending $73,000, and what we actually owe is $380,000. We can't keep doing that. That is how it would relate to the individual family in this country.

The objection was not on the bills. There was no lack of effort on my part to reach out and solve this problem before now and now the minority leader has offered a way to solve the problem on the sanctions for Burma and it is objected to. So not only do we not get to offer amendments in committee, we do not get to offer amendments on the floor. The one thing we need to accomplish today we are not going to accomplish because we don't want to allow amendments.

Because we want to keep doing it the way we have always done it. And the way we have always done it has bankrupted our country and stolen from our children and grandchildren. It is not acceptable anymore.

That is the truth. Everything else is the game that Washington plays. And I will tell my colleagues, I am still willing to work on this. I have a commitment to the Senator from Delaware that next week, if this comes up, I will be the first to offer that amendment and get it out of the way, taking a very short period of time with the Senate. But I want a recorded vote of the Senators in this body that they want to steal the customs user fees for 10 years for just a $200 million pay-for. If that is what you really want to do, then vote that way. But go out and defend it instead of taking something this administration has recommended we cut—which is what I am using to pay for it, something this administration has recommended to pay for it—and vote against what your own President says—here is something we need to eliminate.

I don't get it. The American people don't get it. No wonder we have a 9-percent approval rating.

I yield the floor.

The PRESIDING OFFICER. The Senator from Delaware.

Mr. COONS. Mr. President, I appreciate the opportunity to briefly contribute what I can to this debate.

One of the great honors, as the Presiding Officer knows, in being a freshman is the opportunity to preside. I had the opportunity to preside when the Republican leader came to the floor and spoke to Burma sanctions. So I just wanted to say to the Republican leader that because of that speech, I have familiarized myself with the issue of Burma sanctions that he spoke to earlier. I do think it is important that we move to it. I do think it is important to move forward on it.

But the Republican leader made the comment earlier that he doesn't much understand the other part of the bill, which is AGOA, the African Growth and Opportunity Act. I choose to stand briefly to speak to that because I am the chair of the African Affairs Subcommittee of the Senate Foreign Relations Committee.

Senator ISAKSON and I joined with Congresswoman BASS and Congressman SMITH in twice receiving dozens of Ambassadors from across the continent 3 months ago and 9 months ago as they expressed their grave concern about the thousands of mostly women all across the continent who are losing their jobs as we delay.

The AGOA reauthorization expires in September, and I am grateful for Chairman BAUCUS and for his vigorous pursuit of renewal in a timely fashion. AGOA needs to be renewed promptly, not in September. In part, I believe this is why the administration has insisted on holding together Burma sanctions and this AGOA reauthorization—it is because of the urgency of getting AGOA reauthorized.

It dates back to the Clinton administration. It was first signed into law a dozen years ago. I think it has real importance for our view in Africa, for how the United States is viewed in Africa, for our bilateral relations with more than a dozen countries. I would be happy to answer questions about it.

But we have three different issues here: the concerns the Senator from Oklahoma has raised about the pay-for, and I respect his concerns about budget and budgetary discipline and dealing with our deficit; the concerns the Republican leader has raised about Burma and about sanctions and about our ongoing role as a global leader in pressing for the liberation of people and process in Burma; and the concerns many other Senators and I have shared about timely reauthorization of the African Growth and Opportunity Act. Unfortunately, the three of them intersect in a way that today is preventing us from moving forward.

It is my hope that the Republican leader, the chairman of the Finance Committee, the Senator from Oklahoma, and I can sit down and craft some responsible compromise that allows this to move forward because, if my understanding is correct, it is the concerns of the Senator from Oklahoma that are preventing us from moving forward at this point, and it is the administration's concerns that are preventing breaking apart the Burma sanctions and AGOA sanctions. And there is a third provision relating to CAFTA, if I am not mistaken. So if we could work together in a way that finds a responsible path forward, it is still possible.

There is bipartisan support in the House for the passage of this package. In fact, I believe they were prepared to pass it by unanimous consent earlier this week and only hesitated to proceed because they heard there was a hold here in the Senate.

I would like to work together in a way that can demonstrate to the people of Burma, to the people of Africa, and to the people around the world that this greatest deliberative body on Earth can still work out issues of this scale in a timely fashion. So I offer my willingness to work together to find a path forward either tonight or in the week ahead.

I yield the floor.

The PRESIDING OFFICER. The Senator from Montana.

Mr. BAUCUS. Mr. President, I don't mean to belabor the issue. I see the Republican leader has left the floor. I have just a couple of points.

One, I don't want the impression to be left here that this is a partisan matter. I don't want the impression to be left here that one party favors Burma sanctions and the other doesn't, and the same with respect to AGOA provisions. The fact is, these are both totally bipartisan. Both political parties favor these measures. It is just a matter of working out a way to pass them.

The Senator from Delaware has made a very good point, so let's see if we can work things out within the next couple or 3 days.

The Senator from Oklahoma makes a very valid point, too; that is, sometimes we pay for measures around here with measures that take several years to actually pay for. It is a common practice around here. And to say we have done it once does not necessarily mean it is right.

But I say to my good friend from Oklahoma, who has voted for this kind of measure 11 times, by my count, and once even on the Burma bill, that when we work over the next several weeks and next several months on resolving the fiscal cliff and tax reform, it will be a good opportunity to find ways to reduce our budget deficits, both spending and revenue, and an opportunity to address it in a way that does not do violence to them and that respects the concept the Senator from Oklahoma was mentioning. He has mentioned a

concept that applies not just with respect to customs user fees but for a lot of tax provisions around here, and I think it is something we should talk about and figure out how we want to handle it. But in the meantime, I just suggest that—let's keep talking. There are a few days left here before we leave for the August recess.

I thank my colleagues for working together to try to find a solution.

I yield the floor.

The PRESIDING OFFICER. The Senator from New Hampshire.

GUOR MARIAL AND THE 2012 OLYMPICS

Mrs. SHAHEEN. Mr. President, tomorrow the attention of the world will turn to London as we witness the opening of the 2012 Summer Olympics. Over 10,000 athletes representing 204 nations from around the world will be competing in hundreds of sporting events at the games of the 30th Olympiad. Here in the United States, we will be cheering on the 529 U.S. athletes as they look to bring home the gold for the United States of America. The Olympics no doubt will have countless stories of triumph and disappointment, competition and camaraderie.

I rise today to share the remarkable story of one particular athlete who will be competing this year. His story is one of inspiring triumph of character and spirit. But until just days ago, this Olympian had no flag to compete under. This story is about a talented young runner named Guor Marial whose mere survival in southern Sudan defied the odds. Having escaped the bloodshed and violence in war-torn Sudan, Guor found his way to my home State of New Hampshire as a teenage refugee. Who could have imagined that in just over a decade, Guor would be applying for U.S. citizenship and traveling to London to compete in the Olympic marathon?

Guor was born in a town in what is now part of the fledgling country of South Sudan. Many of his family and friends, including his brother, were killed at the hands of Sudanese security forces. Many more died of starvation or disease brought on by the violence and unspeakable crimes committed by these Sudanese forces.

Before escaping Sudan, Guor was a victim of violence on numerous occasions. As a child, he was kidnapped from his hometown and enslaved as a laborer before eventually finding a way to escape and return to his family. Guor was severely beaten by the Sudanese police and had to spend days in a hospital to recover. Finally, he was able to flee to neighboring Egypt and eventually to the peace and safety of New Hampshire as a refugee seeking asylum.

Guor arrived in my home State of New Hampshire in 2001, almost exactly 11 years ago. He remembers that day well and still considers New Hampshire his home. He lived in Concord, the State capital, moving in with the families of his friends, teammates, and his cross-country coach for 2 years in order to graduate from high school. The contrast between Guor's former life and his new life is stark. In Sudan, he was running in fear for his life. In New Hampshire, he was running for the joy of athletic competition and to be part of a team.

Amazingly, in only his second official marathon, Guor ran fast enough to qualify for the 2012 London Olympics. Given his unique situation, however, it looked as if the bureaucracy would triumph over his bravery and that Guor might not be able to compete because according to the rules of the International Olympic Committee, permanent residents of a country are not permitted to compete on that country's team. As a result, Guor can't compete under the American flag because he is not yet a full citizen. In addition, Guor can't run for the newly recognized country of South Sudan because it is such a new country, it doesn't yet have an official Olympic committee.

The International Olympic Committee suggested that Guor compete as a member of the Sudanese team, and the Sudanese Government extended him an invitation. But Guor rightfully refused, explaining that running for Sudan ''would be a disappointment and an embarrassment to me and the people of South Sudan who died for freedom, including my brother.'' Guor was not comfortable running on behalf of the country that tortured and murdered so many of his family members. That solution would have been cruel and unacceptable.

Fortunately, after some pressure by Refugees International and other friends of Guor who wrote to the International Olympic Committee on his behalf, we received the great news this week that the IOC executive board has decided to make an exception for Guor. He will run in the marathon as an independent Olympic athlete under the great Olympic flag. I want to thank the International Olympic Committee for this very appropriate ruling. In addition, I want to thank the U.S. Olympic Committee, the U.S. Department of State, and the other friends of Guor who worked so hard to make his participation possible.

As he runs under that five-ringed flag, long a symbol of hope for peace in our world, Guor will run with the support of his family, his New Hampshire supporters, Americans everywhere, and his new country, South Sudan. I have a feeling that such support might help him run even faster.

We are so proud of Guor in New Hampshire and proud that in the United States someone who has lived through such tragedy and adversity can start a new life and rise to such incredible heights.

Scott Hamilton, an American Olympic gold medalist, once said, ''Most other competitions are individual competitions. But the Olympic games is something that belongs to everybody.'' No matter the outcome in London, the story of Guor Marial and the adversity he has overcome belongs to everyone. Win or lose, he will stand as a lasting inspiration for people around the globe and as a tribute to the greatness that is the United States of America. I look forward to welcoming Guor home from the Olympics as a winner, regardless of the outcome of the marathon.

I yield the floor.

The PRESIDING OFFICER. The Senator from Colorado.

COLORADO DROUGHT

Mr. BENNET. Mr. President, I am here tonight on a different topic than the Senator from New Hampshire, but I wish to congratulate her on her fine work here. I know she doesn't need or wouldn't want me to say that, but the people of New Hampshire are so lucky to be represented by her. And this is exactly why—a reminder that our Olympic athletes are about to start, I hope, winning gold medals. I suspect they will win the most in this summer's Olympics. We are looking forward to that.

The Senator mentioned marathons, which brought to mind what I want to talk about tonight, which is the farm bill—an elegant segue from one marathon to another. I want to talk about it in the context of the severe drought that is facing Colorado and all of rural America, and I want to acknowledge the administration's ongoing efforts to provide Coloradans with disaster relief during this difficult summer of fires and drought.

We need to pass a 5-year farm bill as quickly as possible to address the challenges we are seeing in farm country. We have done the work to get an agreement on the Senate bill. In fact, we passed the 5-year farm bill in this Senate. It was a strong, bipartisan bill. I would like to thank the Senator from Michigan, DEBBIE STABENOW, and the ranking member of the committee for their incredible leadership in working together, both side of the aisle, never in a partisan way, to produce among other things the only bipartisan deficit reduction that any committee, House or Senate, has produced in this Congress—$24 billion of deficit reduction that has been agreed to by Republicans and Democrats. It ends direct payments to producers, which is one of the most substantial reforms we have seen in agriculture policy in a long time, and it strengthens the conservation title of the farm bill, which is very important to my State and to the West.

Colorado has a $40 billion agriculture sector that extends to all corners of our State. Farming and ranching are two things we do extremely well. The Senator from Iowa is here tonight, and his farmers do it extremely well in Iowa as well.

Producers in Colorado and nationwide are experiencing the worst drought in 50 years. While Colorado is certainly no stranger to water challenges, this year's growing season has been particularly tough—to put it mildly.

According to the U.S. Drought Monitor, nearly our entire State is designated as an extreme drought area. This designation means we are experiencing major damage to crops and pastureland, as well as widespread water shortages. While this designation tells us a lot, we only need to ask the farmers and ranchers about how the dry conditions are threatening their operations.

I met recently with a group of corn growers from eastern Colorado. Take a look at what these farmers are up against. This is Steve Scott's cornfield 18 miles southeast of Burlington, CO, a town of 4,200 people near the Kansas border. This crop—and many others in the region—has withered under long stretches of high temperatures with little or no precipitation to help.

The Department of Agriculture reports that 50 percent of Colorado's corn production is in either poor or very poor condition. The drought has also taken a significant toll on our cattle producers. Colorado is one of America's top beef producers. Right now 75 percent of pastureland in Colorado, approximately 900,000 acres—and I am not sure how that measures up to the Presiding Officer's State, but it is pretty close to that size—is rated as either poor or very poor in condition. Dry pasture and feed shortages have led ranchers to liquidate their herds early, well before they have realized their full size and value.

The Greeley, CO, auction producers' barn is seeing double the sales activity right now as compared to the same time last year because ranchers are selling their cattle below full weight and maturity. They are losing anywhere from $200 to $400 a head.

Next week Carl Hansen of Livermore, CO, is selling 160 of his steers and 90 heifers. On average, each animal will be sold 150 pounds underweight due to the drought conditions. If beef is selling at $1.50 a pound, that is $56,000—actually a little more than that—of lost revenue for Carl Hansen and his family.

The consequences of this drought extend well beyond farm country. The damage to our farms and ranches affect other sectors of the economy—from transportation to energy, from banking to retail. We all know there is nothing Congress can do to stop the drought or prevent the next one from coming, but what we can do is give our farmers and ranchers the tools they need to manage this drought and plan for the future by passing a 5-year farm bill.

We hear a lot about uncertainty in these two Chambers. I can't imagine a set of circumstances creating more uncertainty in a difficult situation than that.

Now we hear that the House leadership is planning a 1-year punt on this whole conversation, one more expression that Washington, DC, has become the land of flickering lights, providing very little opportunity for people to be able to plan and have predictability.

What is wrong with the Senate-passed bipartisan farm bill that had the support of 64 Senators? Sixty-four Senators, Democrats and Republicans. Some people voted against it because they didn't think it was adequate to their region, but this was not a partisan vote. Neither the majority nor the minority vote was a partisan vote. This was the Senate operating as the Senate is meant to operate.

A 5-year bill provides our agriculture community with much needed certainty and predictability, but now it is being held up in the House by politics. Let's be clear: No one is pretending that the farm bill can correct bad weather. Our producers are not waiting on the farm bill to do what they do best. Colorado will continue innovating and increasing productivity, but the last thing on Earth they need is to have Washington's unfinished business hanging around their necks.

A 5-year farm bill will provide producers with a set of tools for managing through this drought and planning for the future. The 1-year bill being discussed over in the House by the leadership doesn't recognize—or is unwilling to recognize—the agriculture community's need to do long-term planning.

Among many other important provisions, the Senate farm bill contains revamped risk management programs like crop insurance, which is what I heard was needed by our farmers, and improvements farmers requested to help manage a severe drought exactly like the one we are going through right now. This is the point of that provision. A 1-year bill doesn't have any of those provisions.

Corn farmers on Colorado's eastern plains could lose 40 percent or more of their revenue this season. We need these reforms and the predictability of the Senate bill. Our bill also contains permanent disaster programs that provide responsible assistance to producers in need. Some of these programs, such as the livestock disaster program, expired in September 2011, almost a year ago. If Congress takes the easy way out and does a 1-year extension, our livestock producers will get no relief—none. This means no disaster assistance for ranchers whose pasture is too dry to feed their cattle.

Who is going to explain to the people selling at the Greeley auction barn why this is not a priority for our Congress in the middle of the worst drought in decades?

The House Agriculture Committee passed a 5-year farm bill with a strong bipartisan 35-to-11 vote. Again, this is not the partisan dysfunctionality we talked about for so many months on this floor. We have two bipartisan bills: One was passed out of committee on the House side with broad bipartisan support, and one was passed on the Senate floor with broad bipartisan support. It is not surprising that I am not the only person who is calling for a long-term extension—a 5-year extension. There are 79 House Members, including 41 Republicans, who wrote to the Speaker last week asking him to bring the long-term farm bill to the floor.

Mr. President, I ask unanimous consent that the letter signed by 79 House Members be printed in the RECORD.

There being no objection, the material was ordered to be printed in the RECORD, as follows:

CONGRESS OF THE UNITED STATES,
Washington, DC, July 20, 2012.

DEAR SPEAKER BOEHNER, MAJORITY LEADER CANTOR, DEMOCRATIC LEADER PELOSI, AND DEMOCRATIC WHIP HOYER: Many current farm bill policies expire on September 30, 2012. The House Agriculture Committee passed H.R. 6083, the Federal Agriculture Reform and Risk Management (FARRM) Act, or the 2012 Farm Bill, on July 12th with a strong bipartisan vote of 35–11. While by no means perfect, this farm bill is needed for producers and those who rely on sound agriculture policy and nutrition programs during difficult economic times.

The House Agriculture Committee has done its work and we now ask that you make time on the floor of the House to consider this legislation, so that it can be debated, conferenced, and ultimately passed into law, before the current bill expires. We need to continue to tell the American success story of agriculture and work to ensure we have strong policies in place so that producers can continue to provide an abundant, affordable and safe food supply.

We all share the goal of giving small businesses certainty in these challenging economic times. Agriculture supports nearly 16 million jobs nationwide and over 45 million people are helped each year by the nutrition programs in the farm bill. We have a tremendous opportunity to set the course of farm and nutrition policy for another five years while continuing to maintain and support these jobs nationwide.

The message from our constituents and rural America is clear: we need a farm bill now. We ask that you bring a farm bill up before the August District Work Period so that the House will have the opportunity to work its will. We ask that you make this legislation a priority of the House as it is critically important to rural and urban Americans alike.

We appreciate your consideration of this request and look forward to working with you to advance the FARRM Act.

Mr. BENNET. They wrote:

The message from our constituents and rural America is clear; we need a farm bill now. We ask that you bring a farm bill up before the August District Work Period.

They went on to say:

We ask that you make this legislation a priority of the House as it is critically important to rural and urban Americans alike.

Representative RICK BERG, a Republican from North Dakota, took to the floor last week and said:

Now is the time for the House to act, the time for the farm bill now.

JO ANN EMERSON, a Republican Congresswoman from Missouri, told reporters that ''there are problems with my farmers who need to make planning decisions.''

We are seeing that exact same uncertainty plaguing our farmers and ranchers in Colorado. Yet here we are again. We have seen this before in Washington. We are pretty good at starting conversations, but we are not very good at finishing them. We are kicking the can down the road once again, but

this is the farm bill, which is a bipartisan effort that rarely, if ever, has been used as a political football around this place.

Three days ago David Rogers wrote an article, which I think accurately describes our dilemma. It was in Politico.

Mr. President, I ask unanimous consent that this article also be printed in the RECORD.

There being no objection, the material was ordered to be printed in the RECORD, as follows:

[From Politico, July 23, 2012]

CONGRESS DELAYS FARM BILL AS DROUGHT SPREADS

(By David Rogers)

To understand how far this Congress will go to kick the proverbial can down the road, consider the farm bill—yes, the farm bill.

In the midst of a severe drought, the House Republican leaders are proposing to walk away from farm states and decades of precedent by not calling up the new five-year plan before the current law expires Sept. 30.

Whatever its flaws, the bill promises $35 billion in 10-year savings from exactly the type of mandatory spending that Congress promised to tackle in last summer's debt accord. But rather than disrupt its political messaging, the GOP would put it all at risk by delaying action until after the November elections.

There's little institutional memory left in the Capitol—or perspective on the accumulation of cans rolling down the road these days. But the farm bill delay is new ground for any Congress.

Never before in modern times has a farm bill reported from the House Agriculture Committee been so blocked. POLITICO looked back at 50 years of farm bills and found nothing like this. There have been long debates, often torturous negotiations with the Senate and a famous meltdown in 1995 when the House Agriculture Committee couldn't produce a bill. But no House farm bill, once out of committee, has been kept off the floor while its deadline passes.

If pushed into November's lame-duck session, farmers will join Medicare physicians whose pay will be running out, idled workers worried about jobless benefits, and very likely, millions of families faced with expiring tax breaks.

For all the backslapping over the recent transportation bill, that measure expires in just 15 months. The Democratic Senate no longer even tries to do 12-month appropriations bills. Already in mid-July—when the floor used to be humming—the ''smart money'' is plotting a stop-gap continuing resolution to get to November or beyond.

Such a CR was once treated as a backstop by the Appropriations committees. Now the practice is so prevalent in all areas of government that the letters might stand for ''Congress Retreats.''

''It's to the point where you almost think you should vote against extensions because they are extensions,'' Rep. George Miller (D–Calif.) told POLITICO. ''If you were looking at the United States from outside, you look and you say, 'What are these people? Fools?' ''

Elections do matter, and there's some logic to letting the voters reshuffle the deck before tackling tough issues. But that's not what's happening here.

The presidential campaigns are already being criticized for lacking all substance. But whoever wins, neither President Barack Obama nor Mitt Romney has shown any appetite for this debate—or even knowledge of farm issues.

The Senate has already approved its farm bill; even if Republicans were to win control in November, the GOP's majority will be so narrow that Democrats will be able to block wholesale changes. In the House, the only certainty about a lame duck is there will be even more unhappy people hanging around.

No, the real reason for Speaker John Boehner (R–Ohio) to delay the farm bill is not because there will be better answers after the election. It's because he doesn't like the answers he sees before.

The farm bill came out of the House Agriculture Committee on a strong bipartisan 35–11 vote July 12. Nearly a year after the August debt accords—and eight months after the November collapse of the deficit supercommittee—it is the closest this Congress has come to enacting real deficit reduction from mandatory spending.

But it's not perfect, and Boehner's Republicans are split regionally and ideologically, with the right demanding still greater savings and a more free-market approach to agriculture policy.

Given Democratic concerns over the depth of the food stamp cuts already made, Boehner says there are not 218 votes for passage. Rather than wrestle with this problem, it's easier to run out the clock with symbolic anti-red tape, anti-tax votes on which the GOP is more united.

Senate Democrats have kicked their share of cans as well. First no spring budget resolution. Then no summer appropriations debate. All under the watch of a majority leader—Sen. Harry Reid (D–Nev.)—who served for years on the Senate Appropriations Committee.

Yet there's something bigger about the farm bill.

Perhaps because it is a five-year event and so fundamental to one bright spot in the economy. Or maybe it's the pounding drought across the country that gives pause. Farmers live by nature's calendar, not continuing resolutions. And by failing to act, Congress can seem even more detached from the real lives of everyday people.

Changes in the Washington press foster this detachment. Major newspapers are more prone to editorials than real reporting on the debate. Regional papers, once the backbone of farm coverage, have closed their bureaus. In the new Capitol trend, some of the most experienced agriculture reporters report to clients—not the public.

The biggest irony may be Boehner himself. The speaker, after all, spent his early years on the Agriculture Committee and prides himself on being a ''regular order'' and prochairman leader. He chastises Obama regularly for doing precisely this: kicking the can down the road.

As if to remind him, Rep. Rick Berg (R–N.D.), a Boehner favorite now running for the Senate, took to the floor Thursday just minutes after the speaker had again ducked farm bill questions at his weekly news conference.

''Now is the time for the House to act,'' Berg told his colleagues. ''The time for the farm bill is now.''

The biggest Republican divisions are also where the greatest savings lie: the commodity and nutrition titles.

Both the House and Senate put an end to direct cash payments to farmers, a long-demanded reform saving about $5 billion a year. The dispute is over how much of that money is reinvested in new subsidies—and where.

The Senate bet heavily on a new shallow-loss revenue-protection program geared to Midwest corn and soybean producers. The House whittles this down to make room for more of a traditional countercyclical program that protects against deep losses but is keyed to government-set target prices—a taboo for free-market types.

Southern rice, peanut and wheat producers stand to do far better under the House approach, but the two bills appear to lunge in opposite regional directions. Corn and soybean growers can almost lock in profits in the early years of the Senate plan. At the same time, the House cotton package costs nearly 20 percent more than what was already viewed as a rich Senate deal. And a $14 per hundredweight target price for rice is higher than what many other crops got, when measured against government data for production costs.

The 13 Southern states are the backbone of the House GOP's majority, contributing 102 votes or more than 40 percent of the conference. This is also where the lines are clearest, not just for crops but also food-stamp savings.

House Agriculture Committee Chairman Frank Lucas (R–Okla.) and the committee's ranking Democrat, Minnesota Rep. Collin Peterson, had hoped to thread this needle by offering a new national eligibility standard for the nutrition program somewhat to the right of Texas's food stamp rules. But for the majority of Southern states, it meant a modest increase from 130 percent to 140 percent of poverty as the high-end income cap—and so it ran aground in the committee.

Peterson, refusing to be discouraged, has plunged back into the fray, trying to find some compromise on food stamps and still hoping that Boehner will relent on moving the farm bill this summer.

''Collin is a CPA by training. He's a numbers guy. He's very focused as a Blue Dog about the budgetary consequences of our actions,'' Lucas told POLITICO. ''I think he's basically on the right track as he's described it to me. The question really comes down to: will we wind up with floor time?''

And himself?

The morning after his late night markup, Lucas sought out Boehner and Majority Leader Eric Cantor (R–Va.) face to face. ''They thanked me, smiled at me and left it at that,'' Lucas said.

He himself is worried—like Republicans in the Senate—that simply passing a short-term extension of the current farm law will not be an easy matter in September. Having spent the better part of a year saying direct payments must end, will Congress want to extend them?

''I'm trying to maintain a good solid working relationship with my leadership,'' Lucas smiles. ''I'm trying to be a positive advocate for why I believe our bipartisan bill deserves floor time.''

''I've alerted staff to be ready to go on a moment's notice, and I will also tell you there are external events that could impact the situation. If this drought continues in the West and Midwest, it could drive members to want to see some action.''

Mr. BENNET. To quote Mr. Rogers:

Never before in modern times has a farm bill reported from the House Agriculture Committee been so blocked.

Never before in modern times. I suspect it is true in ancient times as well, but it has certainly been true in modern times. Rogers tells us that he ''looked back at 50 years of farm bills and found nothing like this.'' He continues:

Farmers live by nature's calendar, not continuing resolutions.

I could never have said it so eloquently myself. He also said:

And by failing to act, Congress can seem even more detached from the real lives of everyday people.

I would not have thought it was possible that this place could seem more detached from the everyday lives of the American people than it already appears to be. We found a way of doing that, and that is by failing to pass this bipartisan farm bill through the Congress in a timely way that is essential for people who are suffering through this kind of drought.

I think Mr. Rogers' observation is exactly right, and I have been on this floor many times before saying the people at home in Colorado—Republicans, Democrats, and Independents—don't identify with the cartoon of a conversation that we are having in Washington, DC, right now. I can't think of a clearer example than the failure to act on this bipartisan piece of legislation. This is legislation that would immediately help people all across our country, all across America, who are struggling today.

Mr. President, think for just a moment about our farmers in Colorado and rural communities just like our communities all across this wonderful country. Our farmers and ranchers are experiencing the worst drought in over half a century. Who is going to look in the eyes of our farmers in Middle America and tell them our dysfunctional politics will prevent this bill from moving forward?

Who is going to tell Steve Scott and Carl Hansen that this bill isn't going to be a priority in the Congress, that we are just going to take our recess and go home for a month not having passed this bipartisan piece of legislation, the only manifestation and example of bipartisan deficit reduction in either the House or the Senate in this entire Congress?

I implore the House to figure out how to come to its senses and pass a 5-year bill along the lines of the bill that was passed out of their committee, and then together we can have a conference and decide how we are going to move this bill forward on behalf of farmers and ranchers all across my State and the United States of America.

I yield the floor.

The PRESIDING OFFICER. The Senator from Iowa.

Mr. GRASSLEY. I didn't come to the floor to speak about the farm bill because I did that yesterday. I want to assure the Senator from Colorado that I listened to everything he said, and I agree with him. That was my plea in maybe a little broader context yesterday in asking that the House of Representatives take up the bill. Also, the House brags, legitimately so, about being fiscally conservative, so I agree with what the Senator from Colorado said. This may be the only opportunity—presumably the only opportunity—to pass a farm bill or any bill that saves money from previous programs of previous years. I compliment the Senator from Colorado.

FREEDOM OF SPEECH

Mr. President, I come to the floor to discuss what I consider a disturbing trend that is occurring in this country. A vicious attack is underway on the right to freedom of speech that is protected by the first amendment. It needs to be highlighted, and hopefully it will stop. Free speech is one of the most important rights that Americans enjoy.

Speech on public issues is the way democracy discusses and debates the important questions of the day. Many great political movements in this country's history depended upon this first amendment right, freedom of speech. Even when Martin Luther King was jailed and his supporters subjected to violence, free speech enabled him to change the views and practices of an entire nation. Today too many government officials seek to shut up people who disagree with them rather than debate those people and debate those issues.

There have been a series of recent incidents to which I want to refer. Consider recently that the Senate Committee on the Judiciary in the past month has held two hearings that prove my point. A hearing was held on a bill that would criminalize supposedly deceptive statements in advance of elections. It would allow the government to criminalize political speech based on its content. It would risk government selectively choosing to prosecute its political opponents. t would allow political candidates to make accusations against their political opponents. So it would chill candidates from speaking.

A few days after our hearing, the Supreme Court's ruling in the Alvarez case confirmed all the free speech problems with that bill. But even after that decision, the Justice Department, to my disappointment, issued a letter in support of the bill. That letter made no mention of any first amendment considerations. I have heard no indication that the committee will not mark up this bill which represents a grave threat to freedom of speech.

This week, the Judiciary Committee's Subcommittee on the Constitution held a hearing on the legislative responses to the Citizens United case. In that decision, the Supreme Court ruled that the first amendment's free speech guarantee protects the rights of corporations and unions to make independent expenditures in support of candidates or on any particular policy issue that they want to speak out on. The ruling has no effect on campaign contributions. There are proposals in this body to amend the Bill of Rights, the first amendment, for the very first time, to allow the government to limit how much candidates can spend on speech and, therefore, the amount of speech that the government will permit. And there are proposed constitutional amendments to prevent corporations and labor unions from spending in elections. To me, this is very serious business that we ought to be raising a red flag about.

It is worth remembering what rule the Obama administration asked the Supreme Court to adopt in Citizens United. The Justice Department argued that the government should be able to ban books that contained even one sentence that expressly advocated the election or defeat of a candidate if those books were published or distributed by a corporation or a union. This administration argued in favor of banning books. In light of the practice of totalitarian regimes of the 20th century, this administration's position on free speech is very astonishing. The Supreme Court quite rightly rejected the argument of the administration on that particular point.

It reminded the news media, which is organized in corporate form for the most part, that the exemption from campaign finance laws is by statute, and one which Congress could remove at any time, threatening freedom of the press. If that were to happen and the Constitution were to allow restrictions on corporate independent expenditures, the guarantee of freedom of the press would be as threatened as freedom of speech.

Then there is another situation, and this deals with the restaurant chain of Chick-fil-A. The owner of that chain is a Christian who has spoken in favor of the value of traditional marriage. The chain has not discriminated against anyone so far as has been reported. The restaurant seeks to expand in Boston and Chicago where presumably it would create new jobs, and in order to get there, it has to meet the permit requirements. However, Mayor Menino of Boston wrote a letter to the company president. He said that because of the owner's ''prejudice statements,'' there would be no place in Boston for the discrimination the company represented. The mayor notified the property owners where the restaurant was to open of his views.

In Chicago, an alderman seeks to deny Chick-fil-A from opening in his ward for the same reason. It is reported that President Obama's former Chief of Staff, now Chicago Mayor Rahm Emanuel, is sympathetic to the alderman's point of view.

Once again, this is a gross violation of first amendment free speech. Government cannot deny a benefit to someone because it disagrees with the applicant's views. This is the fundamental principle of our constitutional democracy.

Voicing support for traditional marriage is not discrimination. That speech is not hate speech. Even if it were, the first amendment protects speech that is unpopular with the government. There is no constitutional speech code that allows banning a hate speech any more than government can ban speech in books.

Finally, the Alvarez decision a few weeks ago affects another first amendment issue pending before this body right now. In the Alvarez case, the Supreme Court struck down the Stolen Valor Act which criminalizes lies concerning winning military medals. It did

so on free speech grounds. I know many of my colleagues desire to pass a new law that will accomplish that goal, and if that law is constitutional, I will probably join them in that effort.

Two bills on this subject are now pending in the Senate. Senator BROWN of Massachusetts introduced the first bill and then Senator WEBB did so after the Alvarez decision. There have been efforts to pass both bills by voice vote.

When the Republicans were asked to move the Webb bill, we were told that all Democrats supported the bill. This is a problem. The Webb bill is clearly unconstitutional based upon the Alvarez decision. It criminalizes some lies about medals that the Supreme Court says Congress cannot criminalize.

For instance, it would prohibit lies in campaigns and in employment, even when those lies would not produce the tangible, material benefit that is necessary to punish them. Yet no Democrat objected to passing the bill without debate. Of course, Republicans could not agree to such a request.

Since he did not have the benefit of the Supreme Court decision when Senator BROWN wrote the bill, right now, because of the decision, and he didn't know about it, Senator BROWN's bill is also unconstitutional. The difference between his bill and Senator WEBB's bill, however, is that Senator BROWN now has a substitute amendment that seems to address the problem in a fully constitutional way. But although Democrats want to pass without debate a clearly unconstitutional bill, somehow they object to a clearly constitutional Brown bill.

These games should stop. I am sure all the Members of this body should be willing to support a single constitutional bill that would reenact the prohibition on lying about whether one is entitled to certain military medals.

In short, this country is facing a disturbing increase in government actions that violate the freedom of speech. That is a vital right of our democracy.

Anyone can stand up for speech with which they agree. The test for government officials and the test for free speech is whether they will allow speech with which they might disagree. They may criticize speech, debate the speech, and seek to change minds. But shutting people up, denying them benefits, passing bills that would put people in jail for exercising free speech rights—these are never allowable under our Constitution. It is time for elected officials to pay greater heed to the oath to support the Constitution.

REPORT BY FORMER FBI DIRECTOR WILLIAM WEBSTER ON FORT HOOD ATTACK

Recently, former FBI Director William Webster was asked to investigate how the FBI performed regarding the attack at Fort Hood by MAJ Nidal Hasan.

Major Hasan's attack killed 12 U.S. soldiers, a Defense Department employee, and wounded 42 others. Following the attack, the FBI conducted an internal review and determined that it had information on Major Hasan prior to that attack. As a result, the FBI Director asked Judge Webster to conduct an independent review and investigation of the FBI's handling of the matter. In short, Judge Webster's commission found that the FBI made mistakes that resulted from a number of problems—some operational, some technological.

Some of these mistakes are extremely concerning given that they are basic management failures. For example, the unclassified report states:

> Many agents and most [task force officers] did not receive training on [FBI computer systems] and other FBI databases until after the FBI's internal investigation of the Fort Hood shootings.

This is clearly unacceptable.

Other problems highlighted include failing to issue Intelligence Information Reports on Major Hasan to the Defense Department; confusion about which FBI office was investigating the lead; failure to interview Major Hasan; along with information technology limitations.

All in all, the Webster report paints a disturbing picture of the FBI. It shows lack of training, failure to follow leads, and continued computer problems. These are the types of problems that, quite frankly, we thought were corrected following the terrorist attacks of 9/11.

Ultimately, Judge Webster issued 18 recommendations for the FBI to implement to prevent future problems such as these. The FBI agreed with these recommendations and has stated they will take action to implement those recommendations.

That is good news, of course. The FBI must implement these recommendations and do it immediately. However, we have a duty to make sure the FBI implements these recommendations and holds people accountable—in fact, hold the FBI accountable—if they don't. The FBI's failure in this case is inexcusable and shakes public confidence in the FBI's ability to combat homegrown terrorism. Basic management problems and investigative failures can't happen, particularly if national security is at stake. If failures of this magnitude occur on high profile national security cases, it makes one wonder what the FBI is doing on other investigations.

Those responsible for these failures should be held accountable. I intend to follow up with Director Mueller to determine what action was taken against those people who didn't do the job in the right and correct way.

JUSTICE DEPARTMENT INSPECTOR GENERAL REPORT

One more report that can't go ignored is a report released this morning by the Justice Department Office of Inspector General. This report examined improper hiring practices within the Justice Department's Justice Management Division. Shockingly, the inspector general found the Justice Department employees openly and flagrantly violated Federal law.

Let me repeat that these employees violated Federal law and the Department of Justice regulations prohibiting employment of relatives, granting illegal preferences in employment, conflict of interest, and misuse of position. Further, employees who were interviewed by the Office of Inspector General were also found to have made false statements to investigators.

This is an example of the Justice Department run wild. It is troubling to me how employees within the Department colluded and schemed to hire one another's relatives in order to avoid rules against nepotism. It is inexcusable, and I can assure my colleagues that we will be looking into this matter.

This wasn't a one-time event, by the way. In fact, the Office of Inspector General pointed out that similar problems existed in 2008. Despite what the Department called ''aggressive action'' to stop this type of behavior back in 2008, it appears nothing has changed.

At the very least, the Attorney General needs to hold these employees accountable with more than just disciplinary action. Laws were broken and false statements were made. The Department can't simply sweep this under the rug. Employees need to be punished because in this town, if heads don't roll, nothing changes.

I yield the floor.

The PRESIDING OFFICER. The Senator from Rhode Island

CLIMATE CHANGE

Mr. WHITEHOUSE. Mr. President, I return to the floor today to give voice once again to the issue I feel will most significantly define this generation of leadership in the United States and around the globe. I rise to discuss the notable, evident changes taking place in our Earth's climate, the relationship between our own activities and the change and the rate of change being observed, and our, so far, forsaken responsibility to address climate change head on and with purpose.

Last month, representatives from world governments, the private sector, NGOs, and other major stakeholders gathered in Rio de Janeiro, Brazil, for the United Nations Conference on Sustainable Development. Marking the 20th anniversary of the 1992 Earth Summit in Rio, this year's conference was nicknamed ''Rio+20.''

So-called sustainable development principles consist of a set of principles and strategies that, when acted upon by the global community, will balance strong economic growth, expansion of just civic and government structures, and environmental protection. Another way to view sustainable development is in the balance of the needs of the present with those of future generations through the fair use of resources.

As Secretary of State Hillary Rodham Clinton said:

> In the 21st century, the only viable development is sustainable development. The only way to deliver lasting progress for everyone is by preserving our resources and protecting our common environment.

One positive aspect of this Rio+20 conference was discussion of the power of economic forces in promoting sustainability. The official Outcome Document adopted by the conference participants entitled ''The Future We Want'' highlights the role of private companies, the private sector—and their close collaboration with governments—in driving sustainable development. It reads in part:

We acknowledge that the implementation of sustainable development will depend on active engagement of both the public and private sectors. We recognize that the active participation of the private sector can contribute to the achievement of sustainable development, including through the important tool of public-private partnerships.

A number of Rio+20's corporate participants have stepped forward to accept this challenge. Many of those global businesses are recognizing that greening their operations is not just good for the environment, it is good for their business as well.

Dell, for example, has committed to reducing its worldwide facilities' greenhouse gas emissions 40 percent by 2015. Dell is a computer technology corporation based in Texas that ranks 44th on the Fortune 500 and employs over 106,000 people. I doubt they made that decision rashly.

Bank of America, based in Charlotte, NC, is number 13 on the 2012 Fortune 500 list and was the first bank to offer coast-to-coast operations in the United States. They have committed $50 billion over 10 years to finance Energy Efficiency, Renewable Energy and Energy Access, and other activities that advance the low-carbon economy.

Marriott has displayed both internal and external efforts by committing to build 10 Fairfield by Marriott hotels constructed to sustainable building standards; as well, pledging $500,000 to help preserve 1.4 million acres of rainforest in the Juma Reserve in the state of Amazonas, Brazil. Marriott ranks first on the Fortune 500 list in the category of the hotel-casinos-resorts industry.

Microsoft has committed to going completely carbon neutral, and will be factoring the costs of carbon output into the company's business operations in over 100 countries.

These companies are just a few examples from the effort that is being undertaken in the private sector to meet our responsibilities to address climate change. As leaders in government, we must recognize that the private sector will not, however, be able to halt climate change on its own. But these commitments do signify that action on climate change does not need to come at the expense of economic growth.

Governments can—and must—provide incentives for sustainable production and consumption. Indeed, the Rio+20 Outcome Document goes on to say: ''We support national regulatory and policy frameworks that enable business and industry to advance sustainable development initiatives taking into account the importance of corporate social responsibility.''

As leaders in the public sector, we have the capacity to establish those effective incentives that can leverage billions in private sector investment into sustainable products and services that support environmental and social improvements. The constructive role that government can play is being recognized not just in capitals around the world but in boardrooms around the world.

Yet, unfortunately, here in Washington, the special interests that deny carbon pollution causes global temperatures to rise, that deny melting icecaps destabilize our climate so that, for instance, regions face extreme drought—as the Senator from Colorado discussed earlier—or outsized precipitation events—that we have seen in my home State of Rhode Island—those special interests in Washington still have a strong hold, and they pretend the jury is still out on climate changes caused by carbon pollution. This is, to be perfectly blunt about it, an outright falsehood.

The fact that carbon dioxide in the atmosphere absorbs heat from the Sun was discovered at the time of the Civil War—1863. Mr. President, 1863 was when the Irish scientist John Tyndall determined that carbon dioxide and also water vapor trapped more heat in the atmosphere as their concentrations increased.

The 1955 textbook, ''Our Astonishing Atmosphere''—from the year I was born—notes that ''Nearly a century ago''—in 1955—''the scientist John Tyndall suggested that a fall in the atmospheric carbon dioxide could allow the earth to cool, whereas a rise in carbon dioxide would make it warmer.''

So this is not something new. This is not something unusual or extraordinary. This is solidly established science.

In the early 1900s, it became clear that changes in the amount of carbon dioxide in the atmosphere can account for significant increases and decreases in the Earth's annual average temperatures, and that carbon dioxide, released primarily by the burning of coal, would contribute to these changes. Again, this is not new stuff. These are well-established scientific principles.

Let's look at the changes we observe in our changing planet. Over the last 800,000 years, until very recently, the atmosphere has stayed within a bandwidth of 170 to 300 parts per million of carbon dioxide—170 to 300 parts per million. That has been the range for 8,000 centuries. By the way, that is a measurement, not a theory. Scientists measure historic carbon dioxide concentrations by locating trapped air bubbles in the ice of ancient glaciers. So we know by measurement over time what the range has been of our carbon dioxide concentration.

What else do we know? Well, we know since the Industrial Revolution, we have burned carbon-rich fuels in measurable and ever-increasing amounts, and that we are now up to 7 to 8 gigatons each year going into our atmosphere. A gigaton, by the way, is a billion—with a ''B''—metric tons. Releasing all this carbon into the atmosphere has, predictably, increased the carbon concentration in our atmosphere. That should not be a difficult proposition, that when you are dumping 7 to 8 billion metric tons of carbon into the atmosphere every year, it raises the concentration of carbon in the atmosphere.

We now measure those carbon concentrations in the atmosphere. We measure them climbing. Again, this is a measurement, not a theory. The present concentration exceeds 390 parts per million. Mr. President, 8,000 centuries between 170 to 300 parts per million, and now we are out over that range, as far as 390 parts per million. In the Arctic, we have actually clipped over into 400 parts per million.

Here is what the Christian Science Monitor said about this:

The Arctic is the leading indicator in global warming, both in carbon dioxide in the air and effects, said Pieter Tans, a senior NOAA scientist.

The Arctic is our leading indicator in global warming, both in terms of the carbon dioxide concentration in the air and the effects of that carbon dioxide concentration.

''This is the first time the entire Arctic is that high,'' he said.

Tans called reaching the 400 number ''depressing,'' and [his colleague Jim] Butler—

Who is the global monitoring director at the National Oceanic and Atmospheric Administration's Earth System Research Lab in Boulder, CO—

said it was ''a troubling milestone.''

''It's an important threshold,'' said Carnegie Institution ecologist Chris Field, a scientist who helps lead the Nobel Prize-winning Intergovernmental Panel on Climate Change. ''It is an indication that we're in a different world.''

''It is an indication that we're in a different world.''

In this article, they make the same point I made a moment ago. I quote the article:

It's been at least 800,000 years—probably more—since Earth saw carbon dioxide levels in the 400s, Butler and other climate scientists said.

So another thing we do pretty regularly around here in business, in the military, in science, is plotting trajectories. It is something that, frankly, scientists, businesspeople, and military folks do every day. There is nothing new here.

When you plot the trajectory for our carbon concentration, the trajectory for our carbon pollution predicts 688 parts per million in the year 2095 and 1,097 parts per million in the year 2195. Mr. President, 688 parts per million in the year 2095, when for 8,000 centuries it has been between 170 and 300 parts per million. So 8,000 centuries at 170 to 300 parts per million, and by the end of this century: 688 parts per million.

To put that 800,000-year figure in perspective, mankind has engaged in agriculture for maybe 10,000 years, maybe a little more. Mr. President, 800,000 years ago, it is not clear we had yet figured out how to make a fire. Millions of years ago goes back into geologic time. Those carbon concentrations—688 parts per million, 1,097 parts per million—those are carbon concentrations that we have not seen in millions of years on the surface of the Earth. And we are headed for them in just a century and a half—two centuries.

As Tyndall determined at the time of the Civil War, increasing carbon concentrations will absorb more of the Sun's heat and raise global temperatures, and experience around the world is proving that is taking place in front of our faces in undeniable ways.

We think often of climate change as happening to our atmosphere, and we think of its effects on our lands because we are land-based creatures. But let me talk for a moment about our oceans.

In April of this year, a group of scientific experts came together to discuss the current state of our oceans. Their workshop report stated this:

Human actions have resulted in warming and acidification of the oceans and are now causing increased hypoxia.

Hypoxia is when there is not enough oxygen trapped in the ocean to sustain life of the creatures that live in the ocean.

Studies of the Earth's past indicate that these are the three symptoms—

Warming, acidification and increased hypoxia—

associated with each of previous five mass extinctions on Earth.

We experienced two mass ocean extinctions 55 million years ago and 251 million years ago. Last year, a paleobiologist at Brown University, whose name is Jessica Whiteside, published a study demonstrating that it took 8 million years after that earlier extinction—the one 251 million years ago—it took 8 million years after that for plant and animal diversity to return to preextinction levels. So that was a pretty heavy-duty wipeout if it took 8 millions years to recover.

Here is the tough part. In the lead-up to these past mass ocean extinctions, scientists have estimated that the Earth was emitting carbon into the atmosphere at a rate of 2.2 gigatons per year for the earlier extinction, and somewhere between 1 and 2 gigatons per year for the second extinction over several thousand years.

Remember how much are we releasing now—7 to 8 gigatons a year. So 2.2 and somewhere between 1 and 2 were the levels that led to those mass extinctions in geologic time, and we are now at 7 to 8 gigatons a year.

As the group of Oxford scientists noted, both of these estimates, the ones for how much was being released in those geologic times, are dwarfed in comparison to today's emission. Our oceans are indeed changing before our very eyes, and anyone who spends time on the oceans or who studies the oceans knows this. The oceans are rising. The oceans are swept by more violent storms. The oceans are getting more acid, affecting already the creatures at the bottom of the food chain, upon which ocean life depends.

It is very hard for a creature to succeed in an environment in which it is becoming soluble. That is what is happening as our oceans acidify, and the small basic creatures at the very bottom of the food chain that live by making their shells can no longer make shells successfully because the water is too acidic.

In the Arctic, we see unprecedented icemelt. The caps are shrinking. Every day it seems we hear about a new record being broken, a new loss of ice cover in the Arctic. In the tropics, we see coral dying. In some places, 80 percent of the coral is gone. I have been to places I can remember live and lively coral reefs, and now we go back and the coral is still there, but it is dead. It is like an abandoned building. Fish can swim around in it, but it is not the fountain of life that a coral reef is supposed to be.

There is a garbage gyre in the Pacific that is estimated to be larger than the size of the State of Texas in which enormous amounts of the plastics we discard are being swept and floating.

We have whales that are poisoned to the point where if they come ashore in Rhode Island on a summer day, if they are hurt or get washed ashore because they are injured, we often end up with whale cadavers in the summers on our coast. When that happens, it is reasonably likely that whale is toxic waste; that if we towed the body back out to the ocean to let it sink and let nature take its course, we would be violating our clean water laws by disposing of toxic waste. If we cranked that whale's body up into the back of a truck and took it to the town dump and chucked it, we would be violating the hazardous waste disposal laws of the State of Rhode Island because we have put so much poison into the ocean that creatures such as whales that live at the top of the food chain have now become so infiltrated with these poisons that they are now swimming toxic waste.

Around here we like to think pretty highly of ourselves. But the laws of physics, the laws of chemistry, the laws of science, these are laws of nature. These are laws of God's Earth. We can repeal some laws around here; we cannot repeal those. Senators are used to our opinions mattering around here. These laws are not affected by our opinions. For these laws of nature, because we can neither repeal them nor influence them, we bear a duty of stewardship, of responsibility to future generations to see and respond to the facts that are before our faces and to see and respond to those facts according to nature's laws.

There is no lobbyist so powerful, there is no secret special interest so wealthy that it can change the operation of those laws. What they have done is to change the operation of our laws, inhibited our ability to meet our duty to respond to the laws of our God-given Earth. We do indeed bear a duty to make the right decisions for our children and grandchildren and our God-given Earth. right now we are failing, shamefully failing, in that duty. We are deluded if we think that somehow we will be spared the plain and foreseeable consequences of our failure to act. Some may hope they will find a wizard's hat and wand with which to wish all this away. That is not rational thinking. If we have a simple obligation to our children and to future generations, it is to be rational human beings and to make rational decisions based on the evidence and the laws of nature. These laws of nature are known. Earth's message to us is clear. Our failure is blameworthy. Its consequences are profound, and the costs will be very high.

I see the distinguished Senator from Alaska who actually brought a wonderful scientist from the University of Alaska who gave one of the better presentations on ocean acidification that I have ever seen as part of our Oceans Caucus.

I yield the floor to Senator MURKOWSKI.

The PRESIDING OFFICER (Mr. FRANKEN). The Senator from Alaska.

EPA

Ms. MURKOWSKI. Mr. President, I have had an opportunity to listen to a few moments of the comments from my colleague from Rhode Island. I clearly share his passion and concern for the oceans. We have been working together as the cochairmen of the Oceans Caucus in the Senate and have had the opportunity to learn from one another on both ends of the country about the significant responsibilities we have, also the great challenges we have, whether it is ocean acidification, whether it is the opportunities we have to ensure that we are good stewards of our water, our land, our air.

It is a challenge I think we face on a daily basis. But I think as we rise to meet these challenges, we recognize that oftentimes within the laws that we have put in place to provide for that level of protection, for that level of oversight and that stewardship, that we may encounter conflict, conflict with the obligation we also have to ensure that the people we represent have an opportunity for good jobs, for a livelihood in a region they call home, that there is a level of balance that we find between our obligation to care for the land, the air, the water, as well as caring for one another.

It is in that vein that I would like to address my comments this afternoon. I would like to speak about certain aspects of what we see within the Environmental Protection Agency and speak specifically to an issue that is

unfolding in my State of Alaska. Clearly, the EPA has important responsibilities to set and also enforce environmental standards. I think we would all agree with that. In the 40 years since EPA was established, our Nation has made dramatic progress in restoring and preserving our environmental resources. I am grateful. I am proud to live in a nation with high environmental standards for the benefit of the land and for the people.

But the process for setting Federal environmental standards, I would suggest, is broken. We are seeing things present themselves not only in my State but around the country. We see in Alaska, day in and day out, that things are not working perhaps as they were designed. So many Alaskans feel the EPA does not ''get'' Alaska.

But the challenges I think we see up North are just examples of many of the problems we see repeated all over the Nation. I would suggest that what we need to see is balance, balance restored at the EPA. There has always been a recognition that the EPA must go about its work in a balanced way.

Back in 1970, there was a memo called the Ash memo, and it listed the origin of the EPA. They stated it this way:

> Sound environmental administration must reconcile divergent interests and serve the total public constituency. It must appreciate and take fully into account competing social and economic claims.

In recent years, EPA has not adequately, let alone fully, taken into account these so-called competing claims such as the genuine welfare of our people and their economic needs. EPA says—and I have had many a conversation with Administrator Jackson in person and before committee, where the statements are made that there is a concern about environmental justice for communities that are historically underrepresented in EPA decisionmaking. The fact is, many of these communities are very frequently the ones that bear the brunt of regressive increases in, for instance in my State, energy and in living costs that are caused by some of these rules we are facing.

When I go home, when I meet with people from around the country, I hear more complaints, more concerns expressed about the EPA than any other Federal agency, bar none. Again and again, I am told the benefits of many of the EPA requirements are uncertain at best but that the cost of the regulations are very real, and they are detrimental to the human welfare.

Today, EPA often seems too eager to impose requirements that are dubious in their health or their environmental benefits but whose main effect may be to penalize or to perhaps even stop commerce or development. So restoring an appropriate equilibrium is vital if we want to have a healthy people, if we want to have a healthy economy.

Today, I would like to speak to one example from my State. There is as it relates to ECA. ECA is a reference to the Emissions Control Area. The EPA was a major proponent of including the ocean off southern and southeastern Alaska in an international emissions control area. This was an effort to reduce emissions from marine vessels through lowering sulfur standards within the fuel.

The purpose of the emissions control areas is to require ships—which, to be very fair, certainly have significant emissions—to do their part to curb pollution. This is absolutely reasonable. The problem we are seeing up north is that EPA never gathered any air modeling data to support the claim that we have a problem from ships that travel up to Alaska. There has been no air modeling data whatsoever. We have requested. There has been none. Moreover, one of the proposals advanced to work with the EPA—and we need to be working with our agencies, as we need our agencies to be working with us—was an offer for an equivalent method to comply with the ECA requirements in North America. We are the only State in the country that is not accessible by road. Folks come and visit us by air and they come in by ship in the summertime. Tourism is big business in Alaska. In Juneau, the ships that are tied up at the docks are utilizing shoreside services so there are no emissions when they are in the community. So one of the proposals that was out there—this equivalency method—would essentially ask for a tradeoff. If we have cruise ships emitting nothing when they are in dock or at shore, offset that against those that would be emitted from vessels out at sea, essentially an averaging. That was rejected by the EPA.

What has made this particularly disconcerting for many Alaskans is that in the EPA's justification they cite a U.S. Forest Service study that purportedly found some evidence that emissions from cruise ships in southeast Alaska could impact the lichen in the mountains above Juneau. We can see the mountains up here in this chart. They are pretty high. There is lichen up on the top. It is kind of a short, mossy, green plant. The report went on to worry that if we have impacted lichen growth in Juneau, it could somehow or other harm the caribou.

Never mind the link that lichen and cruise ship emissions may be very tenuous, there is a bigger problem with EPA's reasoning, and anybody from Alaska would know the problem, which is there are no caribou in Juneau, AK. There are no caribou anywhere in southeastern Alaska. Everyone has seen my pictures before. Alaska is a pretty big State. If we are sitting in Juneau, AK, the caribou herd this report was apparently concerned about is over 1,000 miles away. There are about 1,000 miles between Juneau and where the southern Alaska Peninsula caribou herd cited in the EPA study live—1,000 miles. It would be as if we would make the assertion a cruise ship sitting in Miami might somehow affect the food supply for bears up in the Pocono Mountains north of Philadelphia, PA.

I think we need to look at this and recognize we have a pretty flawed study to begin with, if the suggestion is we need to ensure there are no emissions coming from a cruise ship in Juneau because that is going to impact the lichen which will impact the caribou that don't happen to live anywhere near Juneau—no closer than 1,000 miles away. So applying these new fuel standards to save the lichen in Juneau to feed caribou 1,000 miles from here will mean vessels plying the waters of southeast and south central Alaska—whether they are freight vessels that move just about all our goods or cruise ships that are the lifeblood of our tourist economy—will have to meet the requirement they now burn low-sulfur diesel at levels suggested that are, perhaps, not attainable.

The question I think is fair to ask is: What is the problem with requiring these cruise ships and these vessels bringing goods north to Alaska to meet these standards? What is the problem with this requirement?

The problem is while these ECA requirements may not have a measurable positive effect on human health—or caribou food, for that matter—they will have a material impact on our cost of living. Look at the State of Alaska and the way we get our materials in, the way we get our foodstuffs, our hardware, our lumber. It comes to us over the water. There is some, yes, that comes in by airplane, but guaranteed that is going to cost much more. There are some that can come up from the lower 48 across through Canada and into Alaska that way. But if we want to talk about increased emissions, that is surely one way to do it, to put it on a truck and haul it all the way up here.

So much of our goods come to the State by water. About 85 percent of the goods that come to the State of Alaska come into the Port of Anchorage, which is sitting right there.

What we see with these ECA regs is that ships coming out of a port such as Los Angeles or Long Beach—where my colleague from California hails from, and she is here on the floor now—have hundreds of ships coming in and out every day, but they are not subject to this same emissions control area. They only need to burn this expensive low-sulfur fuel for a very short time until they are out of the ECA. The problem is, when traveling along Alaska's coast to bring those goods up to our State, you are in an area where our air is pretty clean—our air is very pristine—but the entire voyage is within this ECA region. It is all within this emissions control area. So throughout that entire journey they are required to burn the lower sulfur, more expensive fuel.

If this were just going to result in an increase in cost to the cruise lines or to the freight haulers that come up to the State, that might be one thing, but

I think we recognize the economic reality that every dime that is added to the cost of doing business in Alaska is ultimately going to be a dime passed on and shared by consumers.

The State of Alaska recently cited an estimate that these new requirements will increase the shipping costs to the State of Alaska by 8 percent. One might say: Eight percent, that is not that bad. We can live with that. But the problem we face is that in 2015, just around the corner, we will see an even higher standard these vessels will be held to. At that point in time, the suggestion is that costs could be increased by as much as 25 percent. That may be on the high margin, but let's say somewhere between 8 and 25 percent. Again, almost every commodity consumed in our State is transported either by ship or by ship and plane, with the cost of freight adding a significant increase to every item out there.

We are already one of the most expensive places to live in America, and rural Alaska is even more expensive. I check on a weekly basis to find out what Alaskans are paying for their fuel, whether it is in the city of Anchorage or up in Fairbanks or out in Kwethluk or in the villages. I monitor that regularly to see how our villages are faring. In Kotzebue, for instance, this week they are paying about $7.15 for a gallon of gas. I asked that we put a link on our Web site to get some pricing on what we are seeing in our communities as it relates to foodstuffs, things you and I would use in our home here. Here is a package most of us recognize. A 10-pound bag of sugar in Kwethluk is going for $17.25. There is no other store in Kwethluk, other than the Native store, so it is not as if they can go to the Safeway and comparison shop. It is not as if they can get in their car and drive to the city or go to Costco. It just doesn't happen. There are no roads in and out of Kwethluk. You might be able to take an airplane.

A gallon of whole milk costs $30 in Ambler, that is if you can find whole milk or any kind of fresh milk. As a mom who has boys who go through laundry, I am always looking to see what people are paying for laundry detergent. In Venetie, a 100-ounce bottle of Tide goes for $43.50. I had my interns do a little price comparison on Tide. Powdered Tide, 56 ounces, in Anchorage we are paying $9.98. That is a little higher than here in Washington. Washington is about nine bucks. But in Angoon that same box of Tide is $18.33. In Barrow it is $22. In McGrath it is $21. In Bethel it is $21.

So when we talk about increasing the prices in Alaska by 8 percent, 10 percent, 12 percent, possibly 25 percent and you are a mom buying a box of Tide and you are already paying $43, believe me, 8 percent starts to add up real quick. When you are trying to buy a bag of sugar so you can make the food, put up the jam for the winter, and you are paying $17.25 in Kwethluk, I think it is fair to say we are paying attention to what happens when there are cost increases.

EPA mandated low-sulfur fuel is estimated to add $100 million in additional cost to the summer cruise traffic in Alaska. So one might say, if you can afford the price of a cruise, that is not that big of a deal. You increase the price of the ticket and people will live. But what happens is that puts Alaska at a competitive disadvantage when we are talking about where these businesses are going to operate. Fourteen percent of all employment in the State is directly tied to the tourism industry. So if the cruise lines can't fully pass on these increased costs, what they are going to do is move their ships. They will take them to other parts of the world where air quality standards are different, and we will have the loss of seasonal visitors. The money they bring to southeastern Alaska is a huge part of the local economy and also to year-round institutions. In Juneau, our regional hospital is actually able to provide for a higher standard of care, in part, because of the high influx of patients it serves during the summertime.

I would suggest the EPA's one-size-fits-all approach to environmental regulation doesn't always work. We can't quite shoehorn that into in all situations, and we need to be aware of that. Again, when we talk about the concept of environmental justice, we need to make sure when regulations and rules are imposed, we are not hurting the most vulnerable. I would suggest the people in Kwethluk, who are looking at the impact of these regulations and what it is going to mean to them and their village, they are asking: How do we survive? How do we live? The answer isn't for them to move to Washington, DC. That is not the answer. We need to get back to balance.

What is happening now is the State of Alaska has sued the EPA Administrator in Federal Court to stop the new requirements from taking effect. Given the immediacy of the threat these requirements pose to my State, I think the State's move to advance the litigation was the right one. But we shouldn't have to sue our own government in order to get balanced regulation.

Administrator Lisa Jackson has recently acknowledged that applying ECA to Alaska has posed a problem. She recognized that. Unfortunately, we haven't seen anything more beyond those words, and we are still no closer to a solution. These new requirements are set to take effect next week, the initial threshold. I have been raising this issue with EPA for several years, but again we are still working and we have not yet resolved it. I have called on the President himself to marshal the State Department to see if ECA can be amended or some other relief can be found to eliminate at least this one burden.

This is something that is touching Alaskans in a very immediate and a very direct way. Again, we want to ensure our air is clean, that our water is clean. We want to be the good custodians and stewards of our land, and we are. But we need to be able to work with our Federal regulators. I have asked the Administrator and I have asked the President to work with us on this.

TED STEVENS DAY

Mr. President, I know my colleague from California is here to speak, but I would like the indulgence of the body for just 2 more minutes to speak on a little bit of a happy occasion.

TED STEVENS DAY

Mr. President, the day after tomorrow, on Saturday, Alaskans are going to be celebrating Ted Stevens Day. As I travel around the State, whether I am in Fairbanks or down on the Kenai River or up in Bethel, down in Ketchikan, everywhere I go, I am reminded of my good friend and a friend to so many in this body, Senator Ted Stevens.

It was nearly 2 years ago now that we lost Uncle Ted to the tragic plane crash in southwest Alaska. But as tragic as that was, I always stop to remember that that tragedy struck while Ted was doing what he loved to do most, which was enjoying Alaska's great outdoors and going fishing, just being outdoors. His passion for Alaska's unique wilderness, his love for fishing, and his immense affection for the outdoors really embodies the spirit we are now advancing in Ted Stevens Day, and the motto of this day is ''Get Out and Play.''

On the fourth Saturday of July, we join together to celebrate the life and the legacy of a man who was really dedicated to public service, whether it was his days as a pilot in World War II, to the four decades he served with us here in the Senate.

He began working in Alaska long before statehood. When he came here to Washington, DC, to represent us in the Senate, he began a battle for our State that lasted for 40 years. He fought for roads, for buildings, and for infrastructure that new, young States need, as well as many of the programs that are in place today that continue on. He worked to transform not only Alaska but really the rest of the country as well.

It is somewhat coincidental that this Ted Stevens Day coincides with the beginning of the 2012 summer Olympic games in London. So as Alaskans get together to get out and play this weekend under the midnight sun, there are going to be 530 American athletes who will begin to embark on a 17-day Olympic journey Senator Stevens helped to pioneer. It is because of legislation he championed that the Olympic movement in the United States exists as it does today.

Back in 1978, he fought for the passage of the Olympic and Amateur Sports Act. This was later renamed the ''Ted Stevens Olympic and Amateur Sports Act'' in his honor and declared

the U.S. Olympic Committee the centralized body of all Olympic activities in the country and ultimately led to the creation of national governing bodies responsible for the oversight of each individual Olympic sport—a structure that is still in place now. He really was so much an inspiration to the progress and to the development of the Olympic movement here in the United States. Earlier this month, the U.S. Olympic Committee honored Senator Stevens as a special contributor in the Class of 2012 U.S. Olympic Hall of Fame.

We all know Senator Stevens was also a huge proponent of title IX. I think he would be very proud that for the first time in American history, Team USA is comprised of more women than men. I think that would give him a smile. But this feat was made possible by the landmark legislation passed 40 years ago that opened gymnasium doors and leveled the playing field for women and girls across the country.

In Alaska, we very often say that Ted Stevens was larger than life. Today, in discussing this and bringing this up, we recognize that on Saturday we are going to continue a tradition of remembering a man who loved Alaska with a passion. As we go out and bike and hike and fish, I think many will share good memories of an amazing Alaskan, an amazing man, and truly an amazing American.

I thank the Presiding Officer for the opportunity to speak a few minutes about a subject which should, hopefully, bring a smile to many of us.

Mr. President, I yield the floor.

The PRESIDING OFFICER. The Senator from California.

Mrs. FEINSTEIN. Mr. President, I wish to speak on the Cybersecurity Act of 2012. I assume that bill is in order and on the floor.

The PRESIDING OFFICER. The motion to proceed is pending.

Mrs. FEINSTEIN. Mr. President, I come to the floor as the chairman of the Intelligence Committee to, in my own way, indicate the seriousness of the job we are about to begin. I know there is controversy. I know there are differences of opinion. But what people have to understand is that we have breach after breach now, and they have become far more numerous, much more sophisticated, and much more insidious in recent years.

I want to give a number of examples of what is happening out there in the real world, and let me begin by going back to 2008, when the Pentagon's classified military computer networks suffered a ''significant compromise.'' That is according to former Deputy Secretary Bill Lynn in 2010. These breaches are usually classified at the time they happen; therefore, people don't know about them. So all I am going to do is run through unclassified breaches, and even that is beyond comprehension. Former Secretary Lynn also detailed that foreign hackers stole 24,000 U.S. military files in a single attack on a defense contractor in March 2011.

In the 5 months from October 2011 through February 2012, over 50,000 cyber attacks were reported on private and governmental networks, with 86 of those attacks taking place on critical infrastructure networks. Now, that is according to the bipartisan Policy Center's Cybersecurity Task Force. Fifty thousand incidents were the ones that were reported to the Department of Homeland Security, so they represent only a small fraction of the cyber attacks carried out against the United States.

In December 2011, press reports revealed that the networks of the U.S. Chamber of Commerce were completely penetrated for more than a year by hackers. The hackers apparently had access to everything in Chamber computers, including member company communications and industry positions on U.S. trade policies.

In March 2011, NASA's Inspector General reported that cyber attacks successfully compromised NASA computers. In one attack, intruders stole 150 user credentials that could be used to gain unauthorized access to NASA systems.

Another attack at the Jet Propulsion Laboratory that involved China-based Internet Protocol addresses let the intruders gain full access to key JPL systems and sensitive user accounts.

Forty-eight companies in the chemical, defense, and other industries were penetrated during 2011 for at least 6 months by a hacker looking for intellectual property. The cybersecurity company Symantec attributes some of these attacks to computers in Hebei, China.

It became worldwide news when Google alleged in April of 2011 that China had compromised hundreds of Gmail passwords for e-mail accounts of prominent people, including senior U.S. officials.

On March 17, 2011, RSA publicly disclosed that it had detected a very sophisticated cyber attack on its systems in an attempt to obtain data that would compromise RSA's authenticated log-in technology. The data acquired was then used in an attempt to penetrate Lockheed Martin's networks.

Between March 2010 and April 2011, the FBI identified 20 incidents in which the online banking credentials of small to medium-sized U.S. businesses were compromised and used to initiate wire transfers to Chinese economic and trade companies. As of April 2011, the total attempted fraud amounts to approximately $20 million, and the actual victim losses are $11 million.

In October 2010, hackers penetrated the systems of NASDAQ, which sparked concerns about the severity of the cyber threat facing the financial industry.

In January 2011, a hacker extracted $6.7 million from South Africa's Postbank over the New Year's holiday.

In January 2011, hackers penetrated the European Union's carbon trading market, which allows organizations to buy and sell their carbon emissions quotas, and stole more than $7 million in credits, forcing the market to shut down temporarily.

An international computer-crime ring, broken up in October 2010, siphoned about $70 million in a hacking operation targeting bank accounts of small businesses, municipalities, and churches, according to the FBI.

In November 2008, hackers breached networks at Royal Bank of Scotland's WorldPay, allowing them to clone 100 ATM cards and withdraw over $9 million from machines in 49 cities.

In December 2008, retail giant TJX was hacked. The one hacker captured and convicted, named Maksym Yastremskiy, is said to have made $11 million from the hack.

In August 2008, computer networks in Georgia were hacked by unknown foreign intruders, most likely at the behest of the Russian Government because they were coordinated with Russian military actions against Georgia.

In May 2007, Estonian Government networks were harassed by a denial-of-service attack by unknown foreign intruders, most likely again at the behest of the Russian Government because they were part of the worst dispute between the two countries since the collapse of the Soviet Union.

So, as you can see from some of the examples above, for years now, the United States and other countries have been at the receiving end of multiple, concerted efforts by nation-states and non-state actors to hack into our networks. These bad actors are infiltrating our communications, accessing our secrets, and sapping our economic health by stealing intellectual property. They may also be building a capability, if necessary in the future, to wage cyber war. We may not even know until the attack has been launched.

These attacks are sophisticated, and involve hacking techniques that we unfortunately now see quite often. Cyber attacks can come in the form of viruses and worms, malicious backdoors, logic bombs, and denial-of-service attacks, just to name a few.

A groundbreaking unclassified report from November of last year published by the Intelligence Community said cyber intrusions against U.S. companies cost billions of dollars annually. The report named China and Russia as aggressive cyber thieves.

On China, the report said: ''Chinese actors are the world's most active and persistent perpetrators of economic espionage.'' We know that sophisticated attacks from China against financial and technology companies, such as Google, resulted in property theft on a massive scale. Billions of dollars of trade secrets, technology, and intellectual property are being siphoned each year from the United States to benefit the economies of China and other countries.

On Russia, the report said: ''Russia's intelligence services are conducting a

range of activities to collect economic information and technology from U.S. targets.'' I can assure everyone that the classified assessments are far more descriptive and far more devastating.

The examples above are bad enough, but cyber threats are evolving, and I am very concerned that the next wave will come in the form of crippling intrusions against the computers that control powerplants, dams, transportation hubs, and financial networks in these United States.

We have already seen the use of cyber attacks in warfare, when hackers inside Russia reportedly took down the command and control systems in Estonia in 2007. That was 5 years ago, roughly a lifetime in the realm of cyber attack capability.

Senior national security experts from across the political spectrum have sounded the alarm about this threat. For Example, Leon Panetta, at his confirmation hearing to be Secretary of Defense, said:

> The next Pearl Harbor we confront could very well be a cyber attack that cripples our power system, our grid, our security systems, our financial systems, our governmental systems.

Bob Mueller, Director of the FBI, testified before the Senate Intelligence Committee that ''the cyber threat, which cuts across all programs, will be the number one threat to our country.'' We are dealing with the No. 1 threat to the country.

I am pleased to be an original cosponsor of the Cybersecurity Act of 2012 with Senators LIEBERMAN, COLLINS, ROCKEFELLER, and CARPER. I wish to thank them for their tireless work on this legislation over the past several years.

This act has seven titles. Each of them addresses a key gap in our Nation's cyber laws. I wish to take a moment to describe the critical infrastructure provisions in Title I, but I wish to focus most of my remarks on the information-sharing part of the bill, which makes up Title VII.

Title I covers Critical Infrastructure Protection, which means protecting the public and private infrastructure that underpin our economy and our way of life—a big deal. A cyber attack against these networks could open a dam, crash our financial system, or disable the electric grid. It could stop all planes and interrupt the FAA—on and on and on.

Although some critical infrastructure companies have taken action to protect their networks, too many of them have not. It appears that market forces are insufficient for many critical infrastructure companies to adopt adequate cybersecurity practices. Thus, Title I of this bill would create strong incentives for companies to work with the Federal Government to establish standards for critical infrastructure protection.

Let me be candid. Even though the bill makes cybersecurity standards voluntary, I know many Senators still resist this idea. I do not. I would have preferred that this bill include its original critical infrastructure provisions, which would have mandated baseline standards for cybersecurity. But I recognize we have to compromise. I recognize this legislation is a necessary first step to provide some security, and that compromise to the voluntary measures in this bill was necessary. So we have done it. I hope if and when we see a major cyber attack against the power grid, or Wall Street, or a major dam, we won't see this compromise as a mistake.

Other Senators have spoken at length about critical infrastructure and other parts of the bill, so let me move to Title VII, regarding information sharing. This is the part the Intelligence Committee has had something to do with. This title—at least 40 pages of the bill—covers authorities and protections for sharing information about threats to cybersecurity. The information-sharing title addresses one of the main problems I heard from both the private sector and the government about existing laws and business practices when it comes to cyber: that private sector companies and the government know a lot about the cyber attacks against their networks, but this information is so stovepiped that no one is as well protected as they could be if the information were shared. That, I believe, is fact.

As the Bipartisan Policy Center's Cyber Security Task Force recently found:

> Despite general agreement that we need to do it, cyber information sharing is not meeting our needs today.

Title VII addresses this problem. It reduces the legal barriers that hamper a private entity's ability to work with others and the Federal Government to share cybersecurity threat information.

How do we do this? What does that title do specifically? First, it explicitly authorizes companies to monitor and defend their own networks.

Many companies monitor and defend their own networks today in order to protect themselves and their customers. But we have heard from numerous companies that the law in this area is unclear, and that sometimes it is less risky, from a liability perspective, for them to allow attacks to happen than to take additional steps to defend themselves. Can you imagine that? So we make the law clear by giving companies explicit authority to monitor and defend their own networks.

Secondly, the bill authorizes the sharing of cyber threat information among private companies. There have been concerns that anti-trust laws prevent companies from cooperating on cyber defense. This bill, in section 702, clearly says:

> Notwithstanding any other provision of law, any private entity may disclose lawfully obtained cybersecurity threat indicators to any other private entity in accordance with this section.

Third, the bill authorizes the government, which will largely mean (in practice) the Intelligence Community—I hope the DNI—to share classified information about cyber threats with appropriately cleared organizations outside of the government.

Traditionally, only government employees and contractors have been eligible to receive security clearances, and therefore to gain access to national secrets. To put it another way, those with a valid ''need to know'' most security secrets are within the government.

That isn't true, though, for cybersecurity. In this case, we cannot restrict classified information tightly within government—the companies that underpin our Nation's economy and way of life have a ''need to know'' about the nature of cyber attacks so they can better secure their systems.

It is not sufficient for the government to be able to defend itself against an attack. It is also necessary for companies such as Google, or an institution such as NASDAQ, to be able to protect themselves and to use all possible defenses that we can help provide to them.

Under this bill, companies are able to qualify to receive classified information. They will be certified and then able to obtain classified information about what cyber threats to look out for.

Fourth, the bill establishes a system through which any private sector entity—whether a power utility, a defense contractor, a telecom company, or others—can share cyber threat information with the government.

When it comes to cyber, information sharing must be a two-way street. Oftentimes, the private sector has important information about cyber intrusions that the government doesn't possess. After all, the private sector is the one on the frontlines of incoming cyber assault, so companies are often best able to understand the attack.

The private sector should be able to share that information with the government so that the government can protect itself and fulfill its responsibility to warn others about the threat. So let me describe how this bill allows for and encourages that information sharing, and most importantly, let me describe the liability protections that companies receive for doing so.

The Secretary of Homeland Security, in consultation with the Attorney General, the Secretary of Defense, and the Director of National Intelligence, would designate one or more Federal cybersecurity exchanges. We envision that these exchanges would be an existing entity, such as one of the existing Federal cybersecurity centers.

Private companies would share cyber threat information with these exchanges directly. These exchanges must be civilian entities, which is important to a number of Senators. They will have procedures in place to share that information as quickly as possible

with other parts of the government. The information is protected from disclosure under the Freedom of Information Act. It cannot be used in a regulatory enforcement action.

This exchange would serve as a focal point for information sharing with the government. Having a single focal point would establish a single point of contact for the private sector. Otherwise we would have chaos. Some people want multiple points. It is difficult to do and still maintain the security that is necessary.

We think this approach solves the problem. Having a single focal point is also more efficient for the government. It would help eliminate stovepipes, because right now there are dozens of different parts of the government receiving information from the private sector about cyber threats they are encountering. It is all over the map. It would also make privacy and civil liberties oversight easier, which I know interests you, Mr. President. I will describe that in a moment.

Finally, it should save taxpayers money, because it is more efficient to manage—and that has to be a concern—and oversee the operation of one entity versus many entities.

Let me now describe the all-important liability protections that are such a critical part of this.

Section 706 of the bill provides liability protection for the voluntary sharing of cyber threat information with the Federal exchange.

The bill reads:

> No civil or criminal cause of action shall lie or be maintained in any Federal or State court against any entity [that means a company] acting as authorized by this title, and any such action shall be dismissed promptly for . . . the voluntary disclosure of a lawfully obtained cybersecurity threat indicator to a cybersecurity exchange.

That is section 706(a). It is clear as a bell. In other words, a company is immune from lawsuit over sharing cyber threat information with a Federal exchange. The same immunity applies to the following: companies that monitor their own networks; cybersecurity companies that share threat information with their customers; companies that share information with a critical infrastructure owner or operator; and companies that share threat information with other companies, as long as they also share that information with the Federal exchange within a reasonable time. This ''reasonable, good faith'' defense is also available for the use of defensive countermeasures.

If a company shared information in a way other than the five ways I have just mentioned, it still receives a legal defense under this bill from suit if the company can make a reasonable, good-faith showing that the information-sharing provisions permitted that sharing.

Further, no civil or criminal cause of action can be brought against a company, an officer, an employee, or an agency of a company for the reasonable failure to act on information received through information-sharing mechanisms set up by this bill.

Basically—and this is important; please listen—the only way anyone participating in the information-sharing system can be held liable is if they were found to have knowingly violated a provision of the bill or acted in gross negligence.

So there are very strong liability protections for anyone who shares information about cyber threats—which is completely voluntary—under this bill.

Now, what information will be shared with the exchange? Information that should be shared includes—but is not limited to—malware threat signatures, known malicious Internet Protocol, or IP, addresses, and immediate cyber attack incident details.

The exchanges would be able to share this information in as close to real time as possible over networks. That is the only way for the private sector and the government to stay a step ahead of our cyber adversaries.

What kind of information can they share? We define this information in our bill as ''cybersecurity threat indicators.'' We define this term to include only information that is ''reasonably necessary'' to describe the technical attributes of cyber attacks. This is not a license for the government to take in and distribute private citizens' information. Rather, it is narrowly tailored to cover information that relates specifically to a cyber attack.

In addition to narrowly defining what information can be shared with an exchange, our bill also requires the Federal Government to adopt a very robust privacy and civil liberties oversight regime for information shared under this title. There are multiple layers of oversight from different parts of the Executive Branch, including the Department of Justice, the independent Privacy and Civil Liberties Oversight Board, as well as the Congress. I wish to direct Members to the privacy and civil liberties protections on pages 185 through 192 of this bill for the litany of procedures, reviews, and reports that are required.

We have worked closely with several Senators, including the Presiding Officer, Senator FRANKEN, and Senators DURBIN, COONS, AKAKA, BLUMENTHAL, and SANDERS on these protections, and I really thank them all for their efforts in that regard. I think my colleagues have really helped the bill become a better bill.

I would also be remiss if I didn't show my great appreciation of the work and leadership of the majority leader for his unrelenting focus on getting this bill to the floor and making time to have this debate. It is infinitely better having this debate now rather than after a major cyber attack. My greatest worry is that we wouldn't pass something.

The perfect cannot be the enemy of the good. This legislation is unprecedented. It will take some steps. We will find other steps we will need to take. We will need to come back to it and come back to it because technology is moving so quickly.

I think this is as important a bill as I have seen in my 20 years in the Senate. I know what is out there. I know what some other countries are doing. I know what some bad actors are doing. The time has come to protect ourselves and take some action.

I hope we will have the support, and I urge my colleagues to vote for this bill.

Mr. President, I yield the floor and I note the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

The PRESIDING OFFICER. The Senator from Connecticut.

Mr. BLUMENTHAL. I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

HONORING AMBASSADORS TO PAKISTAN AND AFGHANISTAN

Mr. BLUMENTHAL. Mr. President, I am here today to express my sincere appreciation and thanks and admiration to a number of our distinguished Foreign Service officers who were similarly lauded by Senator MCCAIN earlier today. I heard his remarks, and I wish to be associated with them.

I wish to express my thanks to three very brave and able men who have served this country under the most demanding and difficult conditions, requiring huge personal courage as well as insight and strong action. They are Ryan Crocker, who has served as Ambassador to Afghanistan; his deputy who will replace him shortly, James Cunningham; and our Ambassador to Pakistan, Cameron Munter. What they share and what they have given us in these two critical posts is the best of our Nation's public service and foreign service.

I had occasion to meet both Ambassador Crocker and Ambassador Cunningham on a number of visits to Afghanistan and to be briefed by both of them, so I know personally how extraordinarily honest and forthright they are in the insight and intelligence they give to congressional visitors. And many of us have been among those visitors and many of us have met with them, so I know others have had that experience as well. I know them both to be extremely capable and intelligent, thoughtful, and insightful. They understand the complexities of this region, and they have succeeded in maintaining strong relationships with our partners in Afghanistan and Pakistan to the extent they were able to do so amid the most complex and challenging circumstances.

Somehow, in between all of the challenges they faced on the ground day to day, they also welcomed congressional visitors with extraordinary grace and

graciousness and generosity. I was proud to be one of them in visiting both Pakistan and Afghanistan.

I wish to recognize particularly the efforts of Ambassador Munter in addressing the supply chain of IED—improvised explosive device—ingredients, the fertilizer and other chemicals that compose the roadside bombs that have literally caused more than half of our Nation's casualties in Afghanistan. Those ingredients are smuggled, sometimes in broad daylight, across the border from Pakistan. He has worked hard and made a valuable contribution in challenging the Government of Pakistan to do better, and to confront the threat and to ensure interagency coordination between the Department of State and the Department of Defense in confronting and attacking the IED network. He has written to me personally, and I thank him for his commitment to a cause that others have also made a priority, including Dr. Ashton Carter, presently Deputy Secretary of Defense. Together, we worked on this issue and made progress, but so much more must be done to stop the flow of IED bomb-making material across the border which does such horrific, destructive damage to our troops. One need only visit the Bethesda Naval Center to see it firsthand. Our hearts go out to the young men—principally men—and women and their families who are victims of these bombs. Thank you to Ambassador Munter for making it a priority.

I thank Ambassador Crocker likewise for working on this problem as he led the Embassy in Kabul through profoundly and deeply challenging times. When we here in Washington revise our policy toward Afghanistan and as we go through those revisions now, he has adopted and he has carried out policies, and he has served well our national interests, even in the midst of change and challenge.

I welcome Deputy Ambassador Cunningham to his new post. I have worked and been briefed by him. I, in fact, stayed with him in the Embassy. I have seen his keen insight, his quiet, understated manner, and his strength and will.

Indeed, all of these men are men of intellect, but they are also men of action, committed to delivering results to the Nation. They are men of loyalty and courage.

I will just finish on this note. Nobody should underestimate the courage that is required to serve in these positions. Anyone who has visited these countries knows the threat of physical danger is ever-present not only to the brave men and women who serve in uniform in our Armed Forces but to our diplomats who every day put their lives on the line to serve us. So I thank not only them but the thousands of men and women who have served with them in Afghanistan, in Pakistan, and in other countries, at postings in places whose names most Americans can barely pronounce. They have demonstrated the kind of bravery that Ambassadors Crocker, Munter, and Cunningham have every day. They deserve our thanks and our good wishes as they leave their present posts—as Ambassador Crocker retires—and our good wishes for continued success for the sake of their lives and for the sake of our Nation.

I yield the floor and I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

Mr. SCHUMER. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

GUNS IN AMERICA

Mr. SCHUMER. Mr. President, I, like everyone else in America, have followed the terrible tragedy in Aurora, CO. Just awful. I was particularly moved when I read in one of our local papers the bios of the 12 who had died. So many of them were young, in the prime of life, in their late teens and early twenties. So many of them were brave, protecting others—a child, a girlfriend, a friend. I was so upset on reading this, seeing these people's lives snuffed out, just as they had great futures ahead of them—for nothing.

It was the same kind of feeling I had after the World Trade Center—of course, magnified by much more because so many more people died, and I actually knew some of the people who died. But the same senseless killing of innocent people occurred.

Of course, in the days after the tragedy, and as the dust settled—it will never settle for the families whom my heart goes out to—we began our usual discussion about guns in America, and there were many voices on all different sides.

As somebody who has been very involved in these issues, I gave it some thought and wanted to share with my colleagues and with my constituents and my country some thoughts about this.

The question that comes up is: Can we do anything about guns in society? Of course, many would ask: Should we do anything about guns in society? Even the very thoughtful and erudite member of my own party, the Governor of Colorado, said a ban on weapons would not have stopped this tragedy from occurring, in all likelihood.

So I wish to share some of my thoughts briefly.

The bottom line is, maybe we can come together once and for all on the issue of guns if each side gave some. I have thought about this for a while.

As you know, Mr. President, I was the House author—the leader, of course, was my colleague from California—of the assault weapons ban. I am even prouder of the Brady law, where I was probably the leader, and that has saved so many lives.

So the question is: When we were able to pass those kinds of groundbreaking laws, why are we so paralyzed now?

Part of the reason—and this has not been mentioned—is that crime has actually decreased dramatically in America for a whole lot of reasons. I probably do not share the views of some of my colleagues on this side of the aisle as to why it happened. I am a pretty-tough-on-crime guy. But when crime went down, the broad middle that wanted to do whatever it took to stop crime—I remember how it ravaged my city—stopped caring as much because they were safer. That is logical. So they sort of exited the field. Law enforcement, which had been some of our best allies in supporting the assault weapons ban and the Brady law, sort of left the debate. The debate was simply left to those who cared the most, a very small number on the side of more active laws against gun control and a much larger number on the side of those who were opposed.

I know you read in the newspapers: the power of money and the NRA. I have to say this, as somebody who has opposed the NRA and has been written up regularly in their magazines in not the most flattering way, the NRA's main strength is because they have 2, 3, 4 million people who care passionately about this issue, who may not care about other issues, and who are mobilized at the drop of a hat. So when there is a bill on the floor of the Senate which a majority of Americans may support—a majority of Americans support the ban on assault weapons—even people in my State like New York hear much more from the people who are opposed to the assault weapons ban than the people who are for it. Now, 20 years ago, that would not have happened, again, because I think, more than any other reason, crime was so ravaging our communities that average folks would call and complain and worry about too many guns in society, which I think there still are now.

In any case, given that situation, which exists, that the activists, the people who care about this issue the most—not the majority of people—are on the side of no limitations or few limitations on guns, how can we address that balance?

I think there can be a balance. Those on my side who believe strongly in some controls on guns have to acknowledge that there is a right to bear arms. It perplexed many in the pro-gun movement how liberals would read the first, third, fourth, fifth, sixth amendments as broadly as possible, but when it came to the second amendment, they saw it through a pinhole—it only related to militias, which, frankly, is a narrow, narrow, narrow reading of the second amendment.

There were many back then in the 1980s and 1990s in the pro-gun control movement who basically felt there was no right to bear arms. I think in part, because of that, those on the other side of the issue became kind of extreme themselves. Their worry was that the

real goal of the left was not simply to have rational, if you will, laws that might limit the use of guns—what guns could be had, how many clips, who could have them; criminals, the mentally infirm—but, rather, that was just a smokescreen to get rid of guns. And there was enough evidence back in the 1980s and 1990s that people actually wanted to do that.

So if you look at the ads from the NRA and the groups even farther over, the gun owners of America, their basic complaint is that the CHUCK SCHUMERS of the world want to take away your gun, even if it is the hunting rifle your Uncle Willie gave you when you were 14.

I think it would be very important for those of us who are for gun control—some rational laws on guns—to make it clear once and for all that is not our goal, to make it clear that the belief is that the second amendment does matter, that there is a right to bear arms, just like there is a right to free speech and others, and if you are an average, normal American citizen, you have the right to bear arms.

I think if the people who are pro-gun and from the more rural areas, and different than Brooklyn, the city I am from, were convinced that there was a broad consensus even in the pro-gun control movement that there was a right to bear arms, they might get off their haunches a little bit. I think that is important for this part of the compromise. So the Heller decision, which basically said that—and now is the law of the land, but was not until a few years ago—should not be something that is opposed by those who are for rational laws on guns.

I saw that even the Brady organization, that I have worked very closely with—Jim and Sarah Brady helped us pass the assault weapons ban and the Brady law; I have worked with them closely and have known them for decades—but even the Brady organization, which in the past had not had that position, is now beginning to embrace it. I think that is for the good, and I think people should know that.

Once we establish that it is in the Constitution, it is part of the American way of life—even though some do not like that—but once we establish that basic paradigm: that no one wants to abolish guns for everybody or only allow a limited few to have them under the most limited circumstances—this is on a national level—then maybe we can begin the other side of the dialog.

The other side of the dialog is, once you know no one is going to take away your gun, if you are not a felon—your shotgun that you like to go hunting with or a sidearm if you are a store owner in a crime-ridden area—we can then say to those on the other side: OK. We understand that it is unfair to read the second amendment so narrowly and read all the other amendments so broadly, and you have seen us as doing that. But, in response, we would say, and I would say, that no amendment is absolute, and whether it is in reaction to what happened in the 1980s and the 1990s or because of fanaticism, or for maybe fundraising reasons, it seems that too many on the pro-gun side believe the second amendment is as absolute, or more absolute, than all the other amendments. They are taking the converse position to what I mentioned before—the left seeing the second amendment as minuscule, but the right seeing the second amendment as broader than every other amendment.

Certainly, the right believes in antipornography laws. That is a limitation on the first amendment. Certainly, most people in America believe what—I think it was Oliver Wendell Holmes or Louis D. Brandeis who said: You cannot falsely scream ''fire'' in a crowded theater. That, too, was a limitation on the first amendment.

Every amendment is a balancing test. That is what the Constitution has said.

No amendment is absolute or our society would be tied in a complete knot. And so we say to our colleagues, this is not a partisan issue completely. There are some Republicans who are for gun control and some Democrats who oppose it completely. It seems to be more of a regional issue than almost an ideological issue. But we would say to our colleagues from the pro-gun side of things, look, there is a right to bear arms. We are not trying to take guns away from people we do not have any reason to take them away from. But you have to then admit that you cannot be so rigid, so doctrinaire that there should be no limitation on the second amendment.

The Brady law is a reasonable limitation on the second amendment, saying that felons or the mentally infirm or spousal abusers should not have a gun. The Heller decision acknowledged that those kinds of reasonable limitations did not violate the second amendment, just as the Court has recognized they are limitations that do not violate the first amendment, all because it is a balancing test.

So I would argue—and we can all find the balance in different ways—not only is the Brady law a reasonable limitation on the second amendment, it is not interfering with the average person's right to bear arms, but neither are the assault weapons. I know there was an argument between my colleague from California, with whom I agree, and my colleague from Wisconsin, with whom I do not agree: An AR–15 is used for hunting. But I have heard people say you should be able to buy a bazooka or a tank. My view is, the assault weapons ban that was passed, which was a rather modest bill, was less important in saving lives than the Brady law by many degrees. But I would argue it is a reasonable thing to do. A limitation that says you should not be able buy a magazine that holds 1,000 rounds, that is a reasonable thing to do. Rules that say we should be able to trace where a gun originated so we can find those who are violating some of these limitations such as the Brady law—gun shops that do not check your background even though they are required to by law—is a reasonable thing to do. Again, we can debate where to draw the line of reasonableness.

But we might, might, might—and I do not want to be too optimistic here, having years and years of having gone through this—but we might be able to come to an agreement in the middle where we say, yes, there is a right to bear arms, and, yes, there can be reasonable limitations on the second amendment just as there can be on others.

That is the place I suggest we try to go. Maybe, maybe, we can break through the hard ideological lines that have been drawn on this issue. Maybe, maybe, maybe we can tell those who are at the extremes on the far right and the far left that we disagree with you. And maybe, maybe, maybe we could pass some laws that might, might, might stop some of the unnecessary tragedies that have occurred, or, at the very least, when you have someone who is mentally infirm, such as the shooter in Aurora, limit the damage they are able to do. Maybe.

But I would suggest the place to start here is for us to admit there is a right to bear arms, admit the Heller decision has a place in the Constitution, just like decisions that supported the other amendments, and at the same time say that does not mean that right is absolute. That is just a suggestion. I have been thinking about this since I read those horrible articles about those young men and women being killed. I would welcome comments, particularly from my colleagues on the other side of this issue, whether they be Democrat or Republican, on those thoughts.

Just as we have fought over and over and over again on so many issues, and we have gotten into our corners—there may be none that we have gotten into our corners on more than on gun control. Maybe it is time, as on those other issues, to come out of the corners and try, people of good will, who will disagree and come from different parts of the country with different needs, maybe there is a way we can come together and try and try to break through the logjam and make the country a better place.

I yield the floor and I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

Mr. SCHUMER. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

MORNING BUSINESS

Mr. SCHUMER. Mr. President, I ask unanimous consent the Senate proceed to a period of morning business, with

Senators permitted to speak therein for up to 10 minutes each.

The PRESIDING OFFICER. Without objection, it is so ordered.

19TH INTERNATIONAL AIDS CONFERENCE

Mr. DURBIN. Mr. President, I am proud that the 19th biennial International AIDS conference is being held in the Nation's Capital after 22 years of being held abroad.

President Obama was instrumental in bringing the conference back to the United States by announcing in October 2009 that the United States would lift its entry restriction on people living with HIV.

The United States has been the leader in combating the scourge of HIV/AIDS, and it is fitting that this significant meeting of the best and brightest scientists, philanthropists, activists, government leaders, and people living with HIV/AIDS is taking place in Washington, DC.

It is made even more symbolic by the fact that Washington, DC, has the highest rate of AIDS than any city in the Nation.

As we look to ''Turn the Tide Together,'' as the theme of the conference indicates, we must continue to support a number of long-term strategies both at home and around the world, building on the successes we have seen in the past few decades.

Significant scientific breakthroughs have been made this year alone, and we can see investments we have made to fight HIV/AIDS beginning to pay off.

The National Institutes of Health, for example, released a study last fall on the HPTN 052 clinical trial that showed that if newly infected individuals started antiretroviral treatment when their immune systems are relatively healthy, they are 96 percent less likely to transmit the virus to their uninfected partner.

Others report that the cost of treating HIV is four times less than previously thought. And now more than ever, scientists believe that an effective HIV vaccine is within reach.

These are amazing breakthroughs and could reflect the beginning of the end as we work toward an AIDS-free generation.

This past year new infection rates and AIDS deaths decreased. Twenty percent more people had access to antiretroviral therapy worldwide in 2011 than they did in 2010.

These numbers don't appear out of thin air—they correlate to increased investments from the United States and the Global Fund. This is a time when we must continue funding our investments to fight HIV/AIDS.

But let's talk about how we have achieved these amazing results.

President Bush was instrumental in establishing PEPFAR. The President's Emergency Plan For AIDS Relief was initially a $15 billion commitment over 5 years to fight the AIDS pandemic.

Today, PEPFAR is one of the largest health initiatives ever established by a single country and remains critical to saving millions of lives.

PEPFAR is a strongly bipartisan program, and since its inception, it has directly supported nearly 13 million people with access to care and services.

As of 2011, the United States supported lifesaving antiretroviral treatment for more than 3.9 million men, women, and children worldwide.

PEPFAR counseled 9.8 million pregnant women to test them for HIV/AIDS, allowing more than 200,000 babies to be born AIDS-free.

Another key ally in the fight against AIDS is the Global Fund.

The Global Fund was established in 2002 as a public-private partnership, requiring the buy-in of grant recipient countries. These participants must commit to continuing the program and serving its people after the Global Fund grant expires.

This novel approach has proved wildly successful. To date, the Global Fund has supported more than 1,000 programs in 151 countries and provided AIDS treatment to over 3 million people.

The United States must continue to be a leading supporter of the Global Fund.

The generosity of the American people has improved and saved lives, stemmed the spread of HIV/AIDS, and provided medicine, hospitals, and clinics to those who are infected.

Together, PEPFAR and the Global Fund have built health care systems where none existed before and allowed individuals infected with HIV/AIDS to dream of a future.

These programs also ensure that the countries we are working in play a part in helping their own people survive and thrive.

While we have made significant progress in combating HIV/AIDS, we cannot be complacent.

Here in the Nation's Capital, the AIDS rate is higher than in some Sub-Saharan African countries, and infection rates are even growing in some demographics.

In Illinois, 37,000 individuals are living with AIDS, with 80 percent of them residing in Chicago.

Internationally, the gains that we have made could easily be lost; the increase of infections in Southeast Asia, Russia, and the Ukraine—places that have historically had low infection rates is alarming.

If we lose our focus or if international donors stop contributing to key programs, we lose out on the momentum built in recent years to combat this disease.

That is why it is good that this administration continues to push for an AIDS-free generation.

Secretary Clinton announced three new efforts during this week's conference: $15 million in implementation research to identify specific interventions, $20 million for a challenge fund to support country-led efforts to expand services, and $2 million through the Robert Carr Civil Society Network Fund to bolster civil society groups.

Secretary Clinton also noted: ''Creating an AIDS-free generation takes more than the right tools, as important as they are. Ultimately, it's about people—the people who have the most to contribute to this goal and the most to gain from it.'' She is right.

Creating an AIDS-free generation is about working together to help save and improve lives. It is about supporting the individuals and communities that have already made great inroads in addressing this epidemic.

By reaffirming our leadership to initiatives such as PEPFAR and the Global Fund, which support these individuals and communities, we can continue to make a difference. Only then can we truly wish to usher in an AIDS-free generation.

OUR SHARED COMMITMENT TO FIGHT HIV/AIDS

Mr. CARDIN. Mr. President, today I rise to discuss the HIV/AIDS epidemic, the tremendous progress we have made thus far, and the need to do even more if we are going to stop this devastating disease in its tracks.

The fight against HIV/AIDS has been a long one. In more than 30 years, approximately 26 million people have died from AIDS, and there are still an astounding 7,000 new infections every day. But our commitment to combating this disease is making important strides.

In the past decade, new HIV infections fell 20 percent, thanks in large part to the lifesaving antiretroviral treatment we and our partners are making available in every corner of the world that AIDS touches.

We know that relatively healthy people with HIV who receive early treatment with antiretroviral drugs are 96 percent less likely to pass on the virus to their uninfected partners. So treating these individuals not only allows them to live their lives in dignity but is also an important key to prevention.

In my home State of Maryland, the Jhpiego program has spent decades addressing the HIV/AIDS epidemic in South America, Africa, Europe and Asia. Jhpiego has made enormous strides in prevention of mother-to-child transmission, increasing counseling and testing and providing greater access to antiretroviral drugs.

Jhpiego has integrated HIV/AIDS services with tuberculosis, cervical cancer, malaria in pregnancy, family planning and maternal and child health services, to address the problem of co-infection among HIV/AIDS patients and to reach as many people as possible. These integrated services represent the future of our health assistance. We have learned from programs like Jhpiego's what our best practices should be so that we are innovators in prevention, care, and treatment.

I am pleased that Jhpiego and groups like it from across the globe are coming together for this week's AIDS 2012 conference in Washington, DC. This conference is the largest gathering of professionals working in the field of HIV in the world and will bring together more than 20,000 people from more than 120 counties all working together to create a blueprint for combating HIV/AIDS. I can only imagine the exciting new synergies that will develop when so many innovative, committed individuals are in the same room.

Among the presenters are luminaries from the public, private, and multilateral sectors such as President Bill Clinton, U.S. Secretary of State Hillary Rodham Clinton, and former U.S. First Lady Laura Bush, Her Highness Mette-Marit, Crown Princess of Norway, World Bank President Jim Yong Kim, UNAIDS Executive Director Michel Sidib, Sir Elton John, Whoopi Goldberg, and Bill Gates.

This is the first time the United States has hosted the conference in two decades, and I believe it is the right moment for us to be showcasing our strong bipartisan effort to bring the AIDS epidemic to an end.

The United States has long been a leader in the global fight against HIV/AIDS. As chairman of the Senate Foreign Relations Subcommittee on International Development Assistance, I am proud to note that from 2004 to 2010 the United States spent more than $26 billion on bilateral funding to fight AIDS. From my experience leading this subcommittee, I know that dedicated government experts from an array of U.S. agencies are involved in the fight, as are thousands of nonprofits and community organizations.

Yet despite the progress that the numbers and statistics tell us, the story on the ground is still heartbreaking, and now is not the time to rest on our laurels. International anti-AIDS funding has not increased significantly since 2008. In places like the Congo, for example, doctors are only able to supply antiretroviral drugs to 15 percent of the people who need them. Globally, just 8 million of the 15 million treatment-eligible patients in AIDS-ravaged poor regions of the world are getting antiretroviral drugs.

We must do better. We must do better to improve the lives of people living with HIV/AIDS, and we must do better to save the lives of their loved ones.

Some experts believe that ''fatigue and forgetting'' are two of the reasons we have not reached more people. Though we have been working on treating this disease for decades, we still have an overwhelming number of infections to treat.

But the good news is that scientists now believe we have the tools to make serious progress in the fight against AIDS. Scientific advances over the last year have been remarkable, and we can't afford to abandon the fight and to lose momentum now.

In a recent Washington Post article, Michel Sidibe, Executive Director of UNAIDS, the Joint United Nations Program on HIV and AIDS, said, ''The previous generation fought for treatment, our generation must fight for a cure.''

I am proud that in just the last year, the National Institutes of Health has increased spending on cure-related research by $56 million. This is a step in the right direction, and I want to see us do more. I stand with the entire HIV/AIDS medical community in renewing the call to prevent, treat, and cure HIV/AIDS. Let's use the opportunity of this historic gathering to renew our call to work on creating an AIDS-free generation.

2012 OLYMPICS GAMES

Mr. DURBIN. Mr. President, tomorrow evening, hundreds of athletes from across the world will gather in London for the opening ceremonies of the 2012 Summer Olympic games.

Among those marching in the Parade of Nations will be 20 athletes from Illinois.

Making his Olympic debut in the 100-meter butterfly is Tyler McGill, a native of Champaign. After turning in the second-fastest time in the world this year at the U.S. Olympic trials, Tyler will be swimming for a spot at the top of the podium in London.

Lake Forest native and Northwestern Wildcat Matt Grevers is already an Olympic Gold-medalist as a member of the two winning relay teams in Beijing. This year, he'll be swimming for individual Gold—and maybe a world record—in the 100-meter backstroke.

As the son of an All-American, swimming is in Conor Dwyer's blood. After achieving personal bests in every event in which he competed at the trials, the Winnetka native will compete in the 400-meter freestyle as well as a relay at his first Olympic games.

Star diver Christina Loukas was born in Riverwoods, where she began swimming and diving at an early age. Although she moved away from Illinois after high school, Christina remained a Cubs fan and returns to Chicago often.

Chatham's Kelci Bryant will join Christina on the women's diving team as she competes in the 3-meter synchronized diving event. Already a two-time NCAA champion, this will also be Kelci's second Olympics.

Algonquin runner Evan Jager won four Illinois State titles in cross-country and track, but he will be competing in a relatively new sport for him—the steeplechase—at this year's Olympics. He qualified for the team after just a few years training for the grueling event.

Chicago's track and field star Wallace Spearmon, Jr., will be looking for vindication this year in the men's 200-meters—a high-pressured sprint that will include many of the fastest runners of all time.

Dawn Harper, who hails from my own hometown of East St. Louis, will be defending her 2008 Olympic Gold Medal in the 100-meter hurdles in London. She won in Beijing in a thrilling upset and with a personal best time, making her the one to beat in this year's games.

Member of the Fighting Illini and All-American Gia Lewis-Smallwood made her first international team in 2011 after competing in the discus for 11 years. She remained in Champaign after graduating, where she not only trains but also volunteers at the nearby YWCA and with Parkland Community College.

Competing in the men's discus event will be Lance Brooks, a New Berlin high school graduate who attended Decatur's Millikin University, where he played for the men's basketball team.

Growing up in Itasca, Sarah Zelenka tried swimming, soccer, volleyball, and basketball. But it wasn't until she went to college that this naturally gifted athlete found her sport: rowing. She has since won gold at the Rowing World Cup and World Championships and will be looking to add an Olympic medal to that collection in London.

Rowing twins Grant and Ross James have competed next to each other their entire lives and share their biggest fan—their mom. After Ross captured the final seat on the eight-man boat going to London, the twins learned that they had fulfilled their lifelong dream of competing next to each other at the Olympics.

At 6 feet 9 inches, Sean Rooney is a natural for the sport of volleyball. He was named Illinois' Player of the Year in 2001 when he led his high school team, Wheaton-Warrenville South, to an Illinois State championship. He competed in his first Olympics in Beijing, where he helped Team USA to a gold medal. He will help them defend that title this year.

Bob Willis grew up in Chicago and learned to sail on beautiful Lake Michigan. After qualifying for the Olympic games, he returned briefly to Chicago before leaving for London, where ''the first water [his] Olympic board touched was Lake Michigan water.''

Greco-Roman wrestler Ellis Coleman grew up in Chicago's Humboldt Park and joined the wrestling team as a way to stay out of trouble in a rough neighborhood. His signature move is an impressive leap called the Flying Squirrel, which he may employ as he wrestles to win Olympic Gold this year in London.

Growing up in Naperville, Candace Parker was a devoted Chicago Bulls fan. So it wasn't surprising when she began to play basketball herself, leading her high school team to multiple Illinois State championships and becoming the first female high school player to dunk a basketball in a sanctioned game. She has been a member of the USA Basketball Women's National Team since 2009 and helped win Gold for the United States at the Beijing Olympics.

Swin Cash will join her on the women's basketball team. Swin was drafted

into the WNBA after leading her college team to an undefeated 39 to 0 season and her second national championship. She now plays for the Chicago Sky.

Born and raised in Springfield, basketball swingman Andre Iguodala will represent the United States on the 2012 Dream Team, or Dream Team Three. His jersey number is now retired at Lanphier High School, where he was both a star student and athlete.

Star defender on the women's soccer team, Amy LePeilbet grew up in Crystal Lake. Her high school coach at Prairie Ridge remembers her not only for her athleticism but for her work ethic and persistence. She will compete as a member of the U.S. women's soccer team in London.

Each of these athletes has arrived in London as a result of years of perseverance and hard work. They have woken up in the dark for early morning practices and endured aching muscles and sore limbs. They have arrived early and stayed late, spending hours at the gym, on the field, or in the pool training for this moment and their Olympic dream.

I congratulate the athletes from Illinois and every athlete representing his or her country at these Olympic games. I look forward to watching them over the coming weeks as they compete for Olympic Gold.

2012 OLYMPIC GAMES

Mr. BLUMENTHAL. Mr. President, I am honored on the opening day of the 2012 London Olympics to congratulate our U.S. Olympic and Paralympic Teams. Proudly, 16 of our top Olympian athletes hail from Connecticut, including 6 women, who played for our legendary University of Connecticut women's teams and will represent our State and Nation as members of the U.S. women's basketball team.

These athletes will make history on a global stage, representing the United States and sharing personal stories that fuel their drive to win. They have this momentous opportunity and responsibility because they have worked hard, demonstrated unremitting character and integrity, and believed in the power of athletic excellence to bring our nation and the world together.

Six extraordinary UConn alumni will compete as members of the 2012 U.S. women's basketball team: Sue Bird, Swin Cash, Tina Charles, Asjha Jones, Maya Moore, and Diana Taurasi. All six players brought UConn teams to national championships during their college careers. The head coach of the U.S. Olympic team, Geno Auriemma, has led the University of Connecticut teams through many exciting seasons while serving as a tremendous role model and mentor. Both Asjha Jones and Tina Charles currently live in Uncasville and play for the Connecticut Sun. Although the others may no longer list Connecticut as their formal residence, these players remain a part of our lives.

Charlie Cole, Ken Jurkowski, Nick LaCava, Sara Hendershot, and Sarah Trowbridge will compete in London as members of our U.S. rowing team. Mr. Cole grew up in New Canaan, CT, and attended New Canaan High School and Yale University where he rowed for the heavyweight team. He has received many national and international titles, including most recently winning the pair at the 2012 National Selection Regatta number 1 and finishing fourth in the four at the 2011 World Rowing Championships. He has been named USRowing's 2011 Athlete of the Year.

Mr. Jurkowski was raised in New Fairfield and attended New Fairfield High School and Cornell University, where he walked onto the team his freshman year, competed all 4 years, and graduated with a degree in biological engineering. He has also served as a volunteer assistant coach for the University of Texas women's rowing team. In London, he will compete in the single sculls event an event that he placed 11th in during the 2008 Beijing games.

Mr. LaCava is from Weston, CT, and attended Phillips Exeter Academy and Columbia University. Among other distinctions, he placed fifth in the lightweight eight at the 2011World Rowing Championships and placed first at the lightweight eight at the 2011 Head of the Charles Regatta. In London, he will compete in the men's lightweight four.

Ms. Hendershot grew up in West Simsbury Connecticut, only starting to row in 2003 as a high school freshman. Already by 2004 and again in 2005, she won the open eight at the USRowing National Championships. She rowed for Princeton University and graduated in 2010. She will compete in the Women's Pair in London with Sarah Zelenka of Illinois.

Ms. Trowbridge was born in Washington, DC, and is a member of the Potomac Boat Club. She was raised in Guilford, CT, and attended Guilford High School. She rowed at University of Michigan on a scholarship. Most recently among her international and national results, she finished ninth in the double sculls at the 2011 World Rowing Championships and won the double sculls at the 2011 National Selection Regatta No. 2. She cites her parents, coaches, teammates, and Olympic hero, Nadia Comaneci, as inspirations. She will compete in the Women's Double Sculls event.

Craig Kinsley and Donn Cabral will represent the United States in track and field. Hailing from Fairfield, CT, Mr. Kinsley brings his experience at high jump and javelin at Fairfield Preparatory High School and Brown University to the international arena. He won the NCAA title in the javelin event in 2010 and in the same year was named Academic All-American and Northeast Region Field Athlete of the Year by the U.S. Track and Field and Cross Country Coaches Association. At Brown University, he studied geology and economics.

Mr. Cabral was born and raised in Glastonbury, CT. He attended Princeton University, where he received All-American titles in track and field and cross country, and in 2012 won the NCAA title and set the U.S. collegiate record in the steeplechase event. He will compete in the Men's 3000M steeplechase this Olympic games.

Rob Crane will hit the water in sailing. Born in Stamford and raised in Darien, he went on to attend the Holderness School and Hobart College. He continues a family legacy of sailing, joining the ranks of his mother and father, who won world and North American championships, respectively. In 2011, he finished 14th in the International Sailing Association and Federal's Sailing World Championships. This Olympics, he will participate in the men's singlehanded laser dinghy sailing event.

In addition to the successes of these 10 accomplished and inspiring athletes, I wish to recognize all around the world poised to participate in the USA Paralympics. Guided by the U.S. Olympic Committee's Paralympic Military, Veteran, and Community Program, State and local communities have developed important programs to enable individuals with physical or visual disabilities to participate and compete in sports. The growing prevalence of community level sports clubs, such as the paralympic sports clubs, offers disabled Americans the opportunity to come together as a community, share their love of sports, and rally around each other.

Our American competitors are inspirational to athletes and nonathletes of all generations. Athletics and sportsmanship connect us, reaching the core of our humanity. They represent our hopes, dreams, and aspirations. They serve as national and international diplomats, working together as a team to best represent our country. Along with my Senate colleagues, I wish our athletes from Connecticut and around the Nation the best of luck and thank them for their incredible public service as leaders during these Olympic games.

EXTENSION OF THE FISA AMENDMENTS ACT

Mr. LEAHY. Last week, the Judiciary Committee considered S.3276, a bill reauthorizing the surveillance provisions of the FISA Amendments Act of 2008, which is set to expire at the end of this year. The Director of National Intelligence and the Attorney General have both stated that reauthorization of these important national security authorities is the ''top legislative priority of the Intelligence Community.''

After the Senate Select Committee on Intelligence reported its reauthorization bill, I asked for a sequential referral. Senator GRASSLEY joined me in that request. It was for a limited time and had we not completed our markup last Thursday, time might well have expired for this committee to act on it. I was surprised last week and since to be criticized for seeking to improve the

bill within its four corners. I thought that was why we sought the sequential referral, in order to consider and improve the bill where we could.

I worked with Senator FEINSTEIN, the chair of the Select Committee on Intelligence. We came to an understanding and she supported the substitute amendment I offered to shorten the sunset and add more accountability and oversight protections. I thank her for that. I am always willing to work with the Senator from California, who is so diligent in her efforts on the Intelligence Committee. We reached a good compromise and agreement.

I had circulated the core of my amendment, to shorten the sunset, back on July 11, before the bill was to be considered. At the request of Republican members of the Judiciary Committee, the bill was held over. I protected their right to do so under our rules. We finally proceeded to the bill last Thursday, July 19. Despite the delay, no Republicans spoke to me about any potential amendments to the bill.

Instead, the evening before the delayed markup, for the first time, Republican offices circulated scores of amendments. It is unfortunate that there have been mischaracterizations of our committee process. Contrary to the statements of some on the other side, no one was precluded from offering an amendment. In fact, a number were offered by Republican Senators. The committee proceeded to vote on Senator KYL's amendment, for example, to create a new material support of terrorism offense in title 18, and rejected it after Senator FEINSTEIN argued against including it on this important measure, despite her support for the substance of the amendment. We proceeded to vote on Senator LEE's amendment, which was about FISA surveillance, and it, too, was defeated. So despite the misstatements to the contrary, the committee proceeded to consider and reject amendments.

There came a point during our initial 2-hour markup when Senator FEINSTEIN urged that amendments about matters not involving the FISA Amendments Act extension be considered on other vehicles at other times, and moved to table amendments. Those motions prevailed. We have had such motions before and sometimes they succeed.

After 2 hours, as Republican Senators left, we lost a quorum and had to reconvene to vote on reporting the bill as amended to the Senate. I thank those Senators from both sides of the aisle who reconvened. The committee voted to report the measure and was able to do so within the short timeframe of our sequential referral.

The FISA Amendments Act legislation is a top priority of the administration and our intelligence community. We have all acknowledged that. The ranking member acknowledged that it is ''a program vital to our national security.'' A number of Republicans proclaimed last week that they were ready to expedite consideration of the measure and would not offer amendments. Then, when the committee adopted the June 2015 sunset date instead of one of the 2017 dates in other versions of the bill, they changed position and sought to use it as a vehicle for extraneous matters and to offer a number of riders to it that were rejected. I do not understand that logic and why the change in the sunset date or the addition of oversight provisions should change the character of the bill or its importance to our national security. The bill is needed to continue the authority to conduct electronic surveillance of non-U.S. persons overseas under certain procedures approved by the FISA Court.

The Justice Department and DNI have told us:

> [It] is vital in keeping the Nation safe. It provides information about the plans and identities of terrorists, allowing us to glimpse inside terrorist organizations and obtain information about how those groups function and receive support. In addition, it lets us collect information about the intentions and capabilities of weapons proliferators and other foreign adversaries who threaten the United States. Failure to reauthorize Section 702 would result in a loss of significant intelligence and impede the ability of the intelligence community to respond quickly to new threats and intelligence opportunities.

The committee agreed with Senator FEINSTEIN when she asked us not to open the bill up to ''extraneous amendments.'' As it was, the committee considered half a dozen amendments offered by Republican Senators. I appreciated Senator KYL volunteering to have his staff convene a meeting to consider amendments to our terrorist statutes that he does not think will be controversial.

Notably, the vast majority of the amendments filed and offered by the Republicans would not have changed or added a single word to either the underlying bill or the underlying statute. Senator LEE's amendment was the only Republican amendment that dealt in any way with the relevant FISA authorities. That amendment received an up-or-down vote by the committee, and most Republican members voted against it.

Once it became clear that the Republican Senators intended to offer a series of extraneous amendments, Senator FEINSTEIN moved to table amendments that were not germane to her bill. She has that right. I protect the rights of all members of the committee, Republicans and Democrats. Four such amendments were tabled, but notably they were tabled by a vote of the full committee, not simply through a ruling by the chairman or my making up rules, as Republican chairmen have done in the past. Indeed, although a motion to table is typically not subject to debate, I asked the committee's indulgence to permit such discussion. No Senator was cut off from offering amendments or engaging in debate.

It is telling that the two amendments that Senator GRASSLEY offered during the committee's consideration of the FISA Amendments Act had absolutely no connection whatsoever with the provisions of title VII of FISA. The first amendment that Senator GRASSLEY offered would have added the death penalty as a punishment to certain crimes involving weapons of mass destruction. The second amendment that he offered would have required a Department of Justice Inspector General audit of criminal wiretap applications from 2009 to 2010. This amendment may be important to Senator GRASSLEY in the context of the Fast and Furious controversy, but it certainly is not relevant to the FISA Amendments Act. Senator FEINSTEIN moved to table both amendments and the motion carried each time.

Let us be accurate, Republican members of the committee were afforded the opportunity to offer amendments, even ones outside the scope of the legislation. The committee has a process, and we followed that process.

I understand that Republican Senators are disappointed that they were not able to use the FISA Amendments Act legislation as a vehicle to carry other legislation. I am disappointed that, as with so many good bills the committee has reported, there was so little Republican support for a measure that everyone concedes is vital to our national security. Like the Violence Against Women Reauthorization Act, which received no Republican vote on this committee; and the Second Chance Act, which received no Republican votes on this committee after a number of Republican amendments were considered and even though it had been a program strongly supported by Republicans historically; the FISA Amendments Act Sunsets Extension Act was not supported by a single Republican Senator on this committee.

Let me remind Senators, again, that the Director of National Intelligence and the Attorney General have emphasized that the reauthorization of the FISA Amendments Act is the intelligence community's ''top legislative priority.'' I encourage any Senator who has not yet done so to review the classified information that the administration has provided to Congress about the implementation of the FISA Amendments Act. This is a measure that requires serious debate and swift action not partisan bickering or baseless accusations. I sincerely hope that we can set aside the election year posturing and press ahead with consideration of this important national security measure. The American people deserve no less.

FAA SUNSETS EXTENSION ACT

Ms. KLOBUCHAR. Mr. President, on July 19, the Judiciary Committee considered legislation to reauthorize the title VII provisions of the Foreign Intelligence Surveillance Act. These surveillance authorities are vital to our

national security, and it is imperative that they be reauthorized before they expire at the end of this year. The reauthorization bill is narrow in scope, and many amendments were proposed at the committee markup that had little or nothing to do with the reauthorization of FISA. As I stated during the markup, I may have supported or been open to working out a compromise on several of the amendments in other contexts. However, I voted in opposition to all of the extraneous amendments offered because I felt their adoption would threaten the timely passage of the FISA reauthorization bill. That is not a risk I was willing to take.

In particular, as for Senator KYL's amendment to criminalize certain behavior that would reward past terrorist acts and Senator GRASSLEY's amendment to impose the death penalty on terrorists who use weapons of mass destruction, I want to make clear that I strongly oppose the funding of terrorism and I believe that terrorists should be subject to the death penalty. I support the objectives of both of these amendments, but I was concerned that their adoption by the committee could delay or prevent passage of the FISA reauthorization bill. I am prepared to work with Senator KYL and Senator GRASSLEY to address these important issues at a more appropriate time going forward.

I hope that these amendments and others are raised in the appropriate context so they can be adequately addressed.

TRIBUTE TO COLONEL PAUL W. BRICKER

Mr. LEVIN. Mr. President, our men and women in uniform sacrifice much to keep our Nation strong and free. They are well-trained, extraordinarily capable and are some of our country's best and brightest. It is with this in mind that I recognize COL Paul W. Bricker as he retires from the United States Army this week. Colonel Bricker has served our country in uniform for more than a quarter of a century, and I am honored to congratulate him on a long and distinguished military career.

COL Paul W. Bricker has served as the Chief of the Army's Senate Liaison Division since May 2011. As a member of the Secretary of the Army's Office of Legislative Liaison, Colonel Bricker was responsible for advising Army senior leadership on legislative and congressional issues, as well as assisting Senators and our staff on Army matters. It is in this capacity that my Armed Services Committee staff and I have worked closely with Colonel Bricker. Throughout his tenure, he has consistently provided important technical expertise and useful insight on the issues, challenges and opportunities that face our soldiers and their families and has exemplified the highest level of professionalism. I also benefited from Colonel Bricker's organizational diligence and military insights on a number of congressional delegation trips over the past year, including to Afghanistan, Pakistan, Turkey and NATO. The success of these trips were due in large part to Colonel Bricker's careful preparation and adaptability in making course corrections on the fly, often literally.

Colonel Bricker has strong Michigan roots. He is a native of northern Michigan and a proud graduate of Michigan State University, where, upon graduation, he was commissioned as a second lieutenant of Aviation. Colonel Bricker has served in a variety of tactical and operational assignments from platoon to corps level in airborne, air assault, light infantry, and motorized units in the United States, Afghanistan, Iraq, and South Korea. He has commanded in combat with the 82nd Airborne Division at both the battalion and brigade level. Additionally, in 2007, he served as the 82nd Airborne Division's Rear Detachment Commander, and from 2005–2006, as the Chief of Aviation for the Multi National Corps-Iraq.

From 2008 to 2010, Colonel Bricker commanded the 82nd Airborne Division's Combat Aviation Brigade and led them to war on short notice as part of the Afghanistan surge. He assumed no-notice responsibility for the DoD Consequence Management Response Force Aviation Brigade while simultaneously executing Department of the Army Pilot Reset. Once in Afghanistan, his brigade supported more than 40,000 coalition troops in Regional Command-South with lift, reconnaissance, MEDEVAC, and attack aviation. They executed the largest air assault in our nation's history without error or incident, a testament to his exceptional leadership. Colonel Bricker's brigade was commended by the ISAF Joint Command Deputy Commander for his exceptional maintenance and safety record under the most trying combat conditions.

We know that our military personnel don't shoulder the stress and sacrifice of military service alone, and Colonel Bricker is no exception. His wife, Katie, and their three children, Jacob, Jesse and Sophia, have proudly stood by his side, sacrificing time with their husband and father while he fulfills his military commitments.

As he retires, Colonel Bricker leaves behind an impressive record of military service and his counsel, professionalism and expertise will surely be missed. Throughout his service to our Nation, Colonel Bricker has been a shining example for the people of Michigan and the United States, and for this, we offer him our heartfelt thanks. I know my colleagues join me in wishing Colonel Bricker and his family all the best as he begins the next chapter in his life.

22ND ANNIVERSARY OF THE AMERICANS WITH DISABILITIES ACT

Mr. HARKIN. Mr. President, July 26, 1990—22 years ago today was a great day in our Nation's history. When President George Herbert Walker Bush signed the Americans with Disabilities Act, we could see the future before us, full of possibility and opportunity for people with disabilities. It was one of the proudest days of my legislative career.

The Americans with Disabilities Act is one of the landmark civil rights laws of the 20th century—a long-overdue emancipation proclamation for Americans with disabilities. The ADA has played a huge role in making our country more accessible, in raising the expectations of people with disabilities about what they can hope to achieve at work and in life, and in inspiring the world to view disability issues through the lens of equality and opportunity.

In these times, it is valuable to remember that passage of the original Americans with Disabilities Act was a robustly bipartisan effort. As chief sponsor of the ADA in the Senate, I worked very closely with Senator Bob Dole and others on both sides of the aisle. We received invaluable support from President George Herbert Walker Bush and key members of his administration, including White House Counsel Boyden Gray, Attorney General Dick Thornburgh, and Transportation Secretary Sam Skinner. Other Members of Congress also played critical roles in passing the ADA first and foremost, Senator Ted Kennedy; but also Senator ORRIN HATCH, and Representatives Tony Coelho, STENY HOYER, Major Owens, and Steve Bartlett.

Before the ADA, life was very different for folks with disabilities in Iowa and across the country. Being an American with a disability meant not being able to ride on a bus because there was no lift, not being able to attend a concert or ball game because there was no accessible seating, and not being able to cross the street in a wheelchair because there were no curb cuts. In short, it meant not being able to work or participate in community life. Discrimination was both commonplace and accepted.

Since then, we have seen amazing progress. The ADA literally transformed the American landscape by requiring that architectural and communications barriers be removed and replaced with accessible features such as ramps, lifts, curb cuts, widening doorways, and closed captioning. More importantly, the ADA gave millions of Americans the opportunity to participate in their communities. We have made substantial progress in advancing the four goals of the ADA—equality of opportunity, full participation, independent living, and economic self-sufficiency.

But despite this progress, we still have more work to do. Last month marked the 13th anniversary of the

U.S. Supreme Court's decision in Olmstead v. L.C., which held that the ADA requires that people with significant disabilities be given a meaningful opportunity to live and remain in their communities, with the appropriate supports and services, rather than having to live in an institution or nursing home in order to receive the services they need. Yet too many people with significant disabilities still do not have access to these home and community-based long-term services and supports—and we must do more. Last month, following a hearing I chaired to assess the progress we have made on this issue in the various States, I sent a letter to the Governor of each State with information about the variety of new tools available through the Medicaid Program to make it easier to provide community-based services, including the Community First Choice Option and the Money Follows the Person Program. I asked each Governor to let me know by September 7 what they are doing within their State to ensure that the promise of the ADA and Olmstead is being met.

We have made significant progress in the last 22 years in making sure that public transportation options, such as buses, are fully accessible to people with disabilities. But we have not made similar progress on the accessibility of taxicabs. During the past year, there have been major advances in New York City on this issue, and I commend Governor Cuomo and the disability advocates. However, we still have a lot of work to do here in Washington, DC, and in other major metropolitan areas of this country. When I was in London last year, every taxicab was accessible to people with disabilities, through universal design. There is no reason that we cannot work toward this same goal here in the United States.

Yet the most critical challenge we still need to address is the persistently low employment rates among Americans with disabilities.

More than two-thirds of working-age adults with disabilities are not part of the labor force. This is shameful, and we need to do better.

Sometimes a picture is more powerful than any words, so I ask you to look at the chart that I have here. This chart compares the labor force participation rates of working-age Americans in the general population, with the participation rates among women, African Americans, Latinos, and people with disabilities between 1990 and 2011.

Less than 35 percent of American adults with disabilities were in the workforce when we passed the ADA in 1990, and less than 20 percent of this population was in the workforce in 2011. Although our country continues to have employment gaps for women, African Americans, and Latinos, the gap for workers with disabilities is many times the gap for these other groups.

The other noteworthy trend this chart shows is that workers with disabilities often don't benefit even when our economy is doing well. Between 1994 and 2000 and between 2005 and 2007 you can see that while labor participation rates went up for other groups, they were either flat or declining for workers with disabilities.

Since the passage of the ADA we have not made a lot of progress on increasing the employment rate of people with disabilities. This was partly due to the confusion about the requirements of the ADA's employment provisions caused by the U.S. Supreme Court's decisions in the Sutton trilogy in 1999 and the Toyota case in 2002. But in 2008, we passed the ADA Amendments Act which once and for all clarified the definition of ''disability'' and started the clock anew on our efforts to increase employment opportunities for people with disabilities.

But I believe our country is on the verge of major progress on the issue of disability employment. I released a report last week calling on the country to finally make this issue a national priority, because I believe in my heart that we can make substantial progress in the next 3 years. A copy of that report, entitled ''Unfinished Business: Making Employment of People with Disabilities a National Priority,'' is available on the HELP Committee Web site.

I think we are on the cusp of making real progress on this issue for a number of reasons.

First, we have a new generation of young adults with disabilities who grew up since the passage of the ADA, sometimes referred to as the ''ADA Generation.'' These young people have high expectations for themselves. This generation sees disability as a natural part of human experience and does not carry the fears, myths, and stereotypes that lowered expectations for individuals with disabilities in earlier generations.

Along with the ADA generation, we have hundreds of thousands of returning soldiers from Iraq and Afghanistan who do not want their visible and invisible war injuries to prevent them from having a career and supporting their families. These veterans are demonstrating their leadership in our civilian workforce just as they did in service to our country.

In part, to seize on these demographic advantages, I worked with the U.S. Chamber of Commerce to set a goal last year that we increase the size of the disability labor force by over 20 percent by 2015. With the leadership of people with disabilities, the Chamber of Commerce, along with elected officials and businesses like Walgreens and Lowes who have also made this a priority, I think we are at a real tipping point.

In particular, Walgreens has been a leader in employing people with disabilities. I attended a CEO Summit on disability employment at Walgreens' distribution center in Windsor, CT, last month, and saw firsthand how Walgreens built a distribution center designed for a diverse workforce, a distribution center with about half of its employees being people with disabilities, a distribution center that is just as productive as the other Walgreens distribution centers, and is in fact outperforming all of Walgreens' other distribution centers on key indicators like time away from work, turnover, and workplace safety.

Today I hosted a roundtable with many different stakeholders, including Members of the House and Senate on a bipartisan basis, Federal and State government officials, people with disabilities, business leaders, and foundations—all committed to increasing employment opportunities for people with disabilities in competitive employment.

If all of us—Members of Congress, business leaders, employers, and people with disabilities—work together, I believe that we can meet the goal of 1 million new workers with disabilities—and ensure that all individuals with disabilities have real opportunities for employment that meet their goals, interests, and high expectations.

So as we celebrate the anniversary of this great civil rights law, we take time to remember the remarkable progress that we have made in the past 22 years, as well as the progress that we will continue to make—including today.

Today, the Senate Foreign Relations Committee marked up the Convention on the Rights of Persons with Disabilities, CRPD, and approved the treaty on a bipartisan vote of 13 to 6. This brings us one step closer to bringing the convention before the full Senate. I would like to thank my colleague, Chairman KERRY, for considering this convention in such a timely manner, and also Senator MCCAIN for his commitment to this issue. I am proud to support the convention's goal to ensure that people with disabilities have the same rights and opportunities as everyone else.

Americans with disabilities already enjoy these rights at home. However, U.S. citizens with disabilities, including our veterans, frequently face barriers when they travel, conduct business, study, or reside overseas. Ratification of the convention would underscore the enduring U.S. commitment to disability rights and enhance the ability of the United States to promote these rights overseas.

American ratification of the convention would not require us to change any U.S. laws, and the amendments adopted today in committee make this abundantly, explicitly clear. The ADA and disability rights issues have always enjoyed bipartisan support, and passage of the Convention on the Rights of Persons with Disabilities should as well. I am pleased to note the convention is supported by former Senator Dole, the U.S. Chamber of Commerce, 21 veterans groups and countless disability rights advocates.

On July 26, 1990, when he signed ADA into law, President George Herbert Walker Bush spoke with great eloquence. And I will never forget his final words before taking up his pen. He said, ''Let the shameful wall of exclusion finally come tumbling down.''

Mr. President, today, that wall is indeed falling. And we must join together, on a bipartisan basis, to continue this progress.

VA AND NIH JOINT PARKINSON'S DISEASE RESEARCH

Mrs. MURRAY. Mr. President, as chairman of the Senate Committee on Veterans' Affairs, I would like to take a moment to recognize the Department of Veterans Affairs and the National Institutes of Health, NIH, for their research into an innovative surgery that has demonstrated success in improving the stability of muscle movement for veterans with Parkinson's disease. VA and NIH's joint research collaboration regarding deep brain stimulation therapy has furthered the medical community's understanding of Parkinson's disease and will be incredibly valuable to doctors and Parkinson's patients throughout the world.

For many individuals, medication alone is insufficient when it comes to dealing with neurological diseases such as Parkinson's disease. VA and NIH conducted research into an alternative treatment option known as deep brain stimulation therapy to test the long-term outcomes of the treatment. Deep brain stimulation therapy is a surgical procedure that implants electrodes into specific stimulation sites within the brain. These electrodes are then able to send electrical pulses to areas of the brain that controls movement and motor control and helps mitigate the symptoms of Parkinson's disease as well as reduce some of the side effects caused by medication. Thanks to deep brain stimulation therapy, thousands of individuals suffering from Parkinson's disease have experienced a dramatic improvement in their quality of life.

Since deep brain stimulation therapy was approved by the Food and Drug Administration, FDA, as a therapy for Parkinson's disease in the late 1990s, there has been an ongoing debate about which stimulation sites within the brain provide the best and most durable treatment outcomes and how long those results last. To better understand the role that stimulation sites play in deep brain stimulation therapy, VA and NIH conducted a 3-year clinical trial. The trial ultimately found that the benefits gained from deep brain stimulation therapy remained after 3 years and the benefits from the surgery were not dependent by which stimulation site was selected for implantation.

This is the type of research that is crucial to providing the care that our Nation's veterans need and deserve. Thanks to the hard work of VA and NIH researchers, the 40,000 veterans living with Parkinson's disease whom VA cares for along with Parkinson's patients across the world will be better equipped to make informed decisions about their treatment options.

In closing, I commend VA and NIH for their efforts to combat a disease that affects so many of America's veterans.

TRIBUTE TO AMBASSADOR L. BRUCE LAINGEN

Mr. BARRASSO. Mr. President, I rise today to honor an accomplished diplomat and distinguished public servant, Ambassador L. Bruce Laingen. On August 6, Bruce will celebrate his 90th birthday. I want to take this momentous occasion to reflect on his contributions and efforts in support of our Nation. Despite the personal sacrifice, Bruce honorably served the United States with expert skill and dedication throughout his long career.

Bruce was born and raised on a farm in southern Minnesota. He joined the U.S. Navy, and served our Nation during World War II. Bruce received his officer training at Wellesley College in 1943, and attended the University of Dubuque in Iowa for general Naval training. He was a commissioned officer in the Naval Supply Corps. Bruce served in the Pacific with amphibious forces in the Philippine campaigns. After World War II, Bruce graduated from St. Olaf College in Minnesota in 1947. He went on to further his education at the University of Minnesota, where he received a Master's degree in International Relations in 1949.

As a result of his passion and interest in what was happening across the globe, Bruce dedicated 38 years to the Foreign Service. He joined the Foreign Service in 1949, and served this Nation across the world in Germany, Iran, Pakistan, and Afghanistan. The United States was very fortunate to have Bruce serve as U.S. Ambassador to Malta from 1977 to 1979.

In June 1979, Bruce returned to Iran to serve as the U.S. Charge d'Affaires in the wake of the Iranian revolution. Within a few months of his arrival, a group of demonstrators took over the U.S. Embassy in Tehran. The students and militants were protesting the United States' relationship with the government of Iran and the Shah's entry into the United States on humanitarian grounds. On November 4, 1979, Bruce was taken hostage along with more than 60 other Americans. For a total of 444 days, he and 51 other Americans were held hostage in Iran. Throughout the entire ordeal, he worked diligently to protect the hostages and resolve the crisis. He showed true professionalism and strength. In his book Yellow Ribbon: The Secret Journal of Bruce Laingen, Bruce describes his personal perspective and thoughts about the events that took place over those 444 days.

Shortly after Bruce's capture, his wife Penelope ''Penne'' Laingen tied a yellow ribbon around an oak tree on their lawn in Maryland to symbolize her hope for a safe return for her husband and all of the hostages. Penne encouraged others to show their support and determination to be reunited with their loved ones through the use of yellow ribbons. The original yellow ribbon was later donated to the Library of Congress. It is because of her efforts that Penne is credited with founding the yellow ribbon campaign during the Iran hostage crisis.

After his release, Bruce became the Vice President of the National Defense University until he retired from the Foreign Service in 1987. He went on to be the Executive Director of the National Commission on Public Service from 1987 until 1990. Between 1991 and 2006, Bruce was President of the American Academy of Diplomacy.

Bruce continued to share his expertise and knowledge through his efforts on several distinguished Boards of Directors including No Greater Love, A Presidential Classroom for Young Americans, the Mercersburg Academy in Pennsylvania, and the National Defense University Foundation. I had the honor of working with Bruce on the Board of Directors of the Presidential Classroom. He has been a strong advocate for this wonderful program, which encourages students to learn about how their government works and aspire to leadership through public service.

Bruce has received many honors as a result of his brave service to our Nation. He was awarded the Department of State's Award for Valor, the Department of Defense's Distinguished Public Service Medal, the Presidential Meritorious Award, and the Foreign Service Cup.

I am grateful for his willingness to serve our Nation and provide strong leadership in implementing the foreign policy goals of the United States. Bruce, Penne, and their three sons Bill, Chip, and Jim have given so much to our Nation.

CROWDFUNDING

Mr. MERKLEY. Mr. President, I rise today to discuss an issue that I and many of my colleagues are very excited about: crowdfunding, which allows startups and small businesses to harness the power of the Internet to pool investments from ordinary Americans intrigued by their ideas. These ideas can range from revolutionary new technologies to simple projects that can improve communities in need.

If crowdfunding is going to take off, this new market needs to inspire confidence in both investors and small businesses. That is why in December of 2011, I introduced S. 1970 with Senators MICHAEL BENNET and MARY LANDRIEU and in March of this year the bipartisan, compromise crowdfunding amendment with Senators MICHAEL BENNET and SCOTT BROWN. That amendment passed the Senate by a vote of 64 to 35 and was included in the

JOBS Act, which passed the Senate and the House of Representatives and was signed into law by President Obama in April of this year.

In putting this legislation together, I was guided by two goals: 1, enabling this market to work for startups and small businesses and 2, protecting ordinary investors from fraud and deception. Fortunately, in many cases, these goals are aligned. The long-term ability for companies to efficiently raise capital will depend on investors' confidence in the reliability of the marketplace. I believe that the legislation we produced sets the right framework for this marketplace to meet both goals. But, for success to be achieved, this framework must be filled in with smart, effective rules and consistent, conscientious oversight by the Securities and Exchange Commission, SEC, a professional and independent self-regulatory organization, and the State securities regulators.

The SEC is currently in the early stages of the rulemaking process required under the law. I seek to offer these comments today to add to the creative thinking going into that process. I explore several ways in which the law is designed to provide a streamlined and simplified crowdfunding process, as well as provide critical investor protections. I will touch on funding portal regulation, national securities association membership, target amounts, disclosures, accountability, aggregate caps, advertising and promotion, the relationship of crowdfunding to other capital raising, the public review period, the role of State securities regulators, and on-going review and adjustment.

The law provides two regulatory options for firms seeking to provide crowdfunding services. A crowdfunding company under the ''funding portal'' option benefits from streamlined regulatory treatment but must be a neutral platform towards investors. Alternatively, a firm can register as a broker-dealer, in which case it can, through its website or otherwise, provide a broader range of investment guidance to investors. These two options provide a solid foundation for a crowdfunding marketplace with a range of business models.

Because both intermediary vehicles will be repeat players in the crowdfunding marketplace, the rules governing their activities are of paramount importance to the success of the marketplace. Registered broker-dealers are subject to a well-established set of regulations. The registered funding portal structure is, however, a new, streamlined approach. As such, attention should be given to how it can fulfill its promise of a streamlined regulatory approach while also providing the appropriate level of investor protection, as set forth in the law and otherwise.

The CROWDFUND Act is designed so that funding portals will be subject to fewer regulatory requirements than broker-dealers because they will do fewer things than broker-dealers. Among other limits, the law prohibits funding portals from engaging in solicitation, making recommendations, and providing investment advice. Relative passivity and neutrality, especially with respect to the investing public, are touchstones of the funding portal streamlined treatment. The SEC will, of course, have to establish boundaries, and I encourage the Commission to consider several points:

Provided that funding portals are not subject to financial incentives that would cause them to favor certain companies or otherwise create a conflict of interest, funding portals should be able to exclude prospective issuers from their platform, whether that exclusion is based on the size of the offering, the type of security being offered, the industry of the business, the subjective quality of the issuer, the amount that the issuer would charge for its securities, e.g., the pricing of shares based on an evaluation of the company's potential, or the interest rate on a debt security given a certain risk profile of the issuer as analyzed by the funding portal, or almost any other reason, including at the discretion of the platform. In short, a funding portal should not be forced, directly or indirectly, to conduct a crowdfunding offering of an issuer it does not have faith in or on terms it does not believe should be made available to its customers.

Subject to such limits as the SEC determines necessary for the protection of investors and the crowdfunding issuers, funding portals should be able to provide, or make available through service providers, services to assist entrepreneurs utilizing crowdfunding, including, for example, providing basic standardized templates, models, and checklists. Enabling them to help small businesses construct simple, standard deal structures will facilitate quality, low-cost offerings. If necessary, streamlined oversight of these may be appropriate, for example, by the relevant national securities association.

Funding portals should be able to highlight for investors, such as through searches, requested email alerts, or profile ''matches,'' issuers according to objective criteria for example, geographic, industry, trending, or not trending, amount an investor wants to pay for a security, or interest rate desired, or randomly.

Funding portals should be able to provide relevant factual information from third parties. For example, in the context of the sale of debt securities, this could be information from credit bureaus regarding the creditworthiness of issuers and their backers.

It is important to remember that nothing in the CROWDFUND Act prevents or limits a person independent of the funding portal from providing recommendations or investment advice to their clients. For example, Community Development Financial Institutions, CDFIs, with their mission-driven mandate and economic empowerment experience, may offer valuable insight for investors seeking to identify healthy, community-based investments.

Some have argued that discretion-based curation, such as highlighting certain companies on a home page for all investors, is important to the success of crowdfunding. However, the activity also comes very close to the line of making recommendations or providing investment advice, which are not permitted owing to the reduced duties that funding portals have compared to broker-dealers. Some of the CROWDFUND Act's streamlining was precisely to enable small companies to successfully raise capital at modest cost, but some of those duties are also important investor protections. The SEC should carefully weigh these concerns and adopt practical, easy-to-manage solutions that facilitate successful crowdfunding for company, investor, and platform.

For example, it should be carefully considered whether organizing of the presentation of companies on the homepage facilitates success, especially by less sophisticated users, and so should be permitted. Of course, the funding portal should not match specific investors with specific companies and must not be compensated in a way that would cause them to favor certain companies or otherwise create a conflict of interest.

Indeed, some argue that discretion-based curation is essential to prevent fraudsters from gaming an objective system. On the other hand, some vigorously context this point and identify it as creating a serious risk for pump-and-dump schemes. One of the reasons I feel regulatory supervision of this space is so important—and fought for it so vigorously during the CROWDFUND Act debate—is because of the professional expertise regulators bring to addressing difficult technical issues. In short, I urge the SEC and the relevant national securities association to consider competing views like these carefully. It should be remembered that crowdfunding comes with a number of investor protections, including the aggregate cap, and so may provide some space for modest experimentation, especially when done in partnership with investor protection advocates and industry participants acting in good faith, and with adjustments made based on actual performance and measurable data.

The SEC is and should feel fully empowered by the law to take actions to protect investors and this is essential, especially at the early stages, when reputational risk to the crowdfunding market is very high. At the same time, I encourage it to approach this marketplace with a spirit of smart, careful experimentation and regular review and adjustment.

In addition, I encourage the SEC to move swiftly to address potential concerns about timing for the registration

of potential funding portals so that they can be ready to go when crowdfunding goes live.

The legislation requires firms offering crowdfunding services to join a national securities association registered with the SEC, also known as a self-regulatory organization, SRO. The vision of the SRO as a genuine regulatory entity owes much to the leadership of SEC Chairman William O. Douglas, the ''sheriff of Wall Street'' during the Great Depression, who believed the SEC had a duty to establish strong regulation in the public interest but that Wall Street itself was well positioned—and should be obligated—to participate in the maintenance of high standards of conduct. Accordingly, any such association must be strictly independent and thoroughly professional, with a strong mandate to operate in the highest forms of public interest and for the protection of investors.

The legislation does not foreclose funding portals from developing their own association. After consulting with the SEC and the Financial Industry Regulatory Authority, FINRA, they may indeed decide such an association would better serve their goals of a professional, independent, high-quality SRO. Setting up an SRO is not easy, though, and it may also make practical sense for funding portals to tap into the architecture already present in FINRA. To facilitate that, I encourage FINRA to work with new funding portals to keep bureaucracy, paperwork, and fees to a minimum, and to ensure funding portals can meaningfully participate in FINRA governance.

Moreover, I urge FINRA to act quickly and in close coordination with the SEC to address potential timing concerns that may exist with respect to the relationship between registration and membership of funding portals and the effective date of crowdfunding. Prospective funding portals should not be disadvantaged in their ability to compete in the initial stages of the crowdfunding marketplace.

The law says companies can only access investor funds once they have raised an amount ''equal to or greater than'' their target amount. The goal of this provision is to ensure that disclosures provided are connected to the target amount—and any higher amount—while also enabling companies which attract more interest than they had expected to obtain the additional funds raised. For example, if an issuer sets its target amount at $50,000 and discloses that it needs the $50,000 for a set of ovens for a vegan bakery, if it only raises $35,000, an investor would have no way of knowing what the company would do with the money—and this is not permitted. However, if the issuer discloses it would buy a small oven if it raised $50,000 and a higher-capacity oven if it raised $70,000, then that would give investors confidence that funds raised and distributed would go to their disclosed use. In short, the disclosures should be tied to the target amounts being raised, and issuers should provide some level of disclosure for how they will use funds above some reasonable percentage beyond their original target.

The law puts in place aggregate caps on an individual's crowdfunding investments in a given year. Without aggregate caps, someone could in theory max out a per-company investment in a single company and then repeat that bet ten, a hundred, or a thousand times, perhaps unintentionally wiping out their entire savings. The challenge is that crowdfunding is a new framework to provide small companies, including many start-ups, opportunities to raise capital. The risks that are present in this space are not amenable to ordinary means of mitigation through diversification. Angel and venture capital funds, whose mission is to invest in the start-up sector, tend to invest in perhaps one out of one hundred opportunities presented and assume that ninety-five percent of investments will fail entirely. Their profits commonly emerge out of only a handful of big winners. Even with the investor education mandated under the law, ordinary investors might not fully appreciate these risks. Aggregate caps can help address this problem.

Because caps scale up as investors can bear greater risk, an important investor protection is the cap—$2000, to be adjusted for inflation—for persons of lower income. One way to ensure that the investor protection inherent in the scaled approach is meaningfully implemented might be to only require persons seeking to qualify for the higher investment amounts make showing regarding their income, but then make that showing slightly higher than simply ''checking a box.'' This approach could protect less sophisticated investors from opting into the higher limits accidentally or due to potentially misleading promptings from a less scrupulous intermediary, while retaining ease of use for the majority of participants utilizing the default amount of $2000.

Some have expressed concern about how to implement the aggregate amounts across platforms. A data sharing regime is one way to do that, but the SEC might also consider whether to pair it with a presumption that ordinary investors that remain within an amount below the default aggregate, for example $500, on any one platform are also presumed compliant across other unaffiliated platforms. This streamlining may be particularly useful for those seeking to make small investments and for those that want to engage in community-based crowdfunding, including those serving the CDFI community.

As the market develops, the SEC should carefully evaluate how these caps are working from perspectives of investors, issuers, and intermediaries.

The bipartisan Senate approach to crowdfunding provides critical disclosures that should help investors make intelligent investment choices. These include core financial information, basics about the business of the issuer, information about major owners, and other key basics any investor needs to know before investing. Disclosures should be designed specifically for the crowdfunding market, enabling start-ups and small businesses to present basic, accurate information appropriate to the amount of money being put at risk by each investor and raised overall by the issuer.

With respect to financial information, the law allows companies raising smaller amounts of money to provide financial information appropriate to the amount of capital being raised—but all companies must provide something. If, for example, an issuer wants to raise $90,000 to develop a prototype project but it is a new company without any previous revenue, that is fine—under the law, it just has to, for example, certify that the company has not yet filed tax returns and provide a CEO-certified set of financial statements displaying the appropriate zeroes. I want this process to work for all kinds of startups and be reasonably tailored to the amount of capital being raised.

The law mandates strong disclosures about capital structure and risks of dilution. Crowdfunding is available for both equity and debt securities, but the more complex the security or capital structure is, the greater the need is for strong disclosure. The goal with the strong disclosure mandate in the law to push issuers towards easy-to-understand, investor-friendly approaches, while also permitting more complex approaches if the appropriate disclosures are made. It was envisioned that the SEC might even adopt safe harbors for simple, investor-friendly structures. It may wish to convene an advisory committee specifically designed to evaluate these issues, as well as also to seek input from the Office of the Investor Advocate.

The legislation also provides for annual reports by issuers to investors. This should be a similarly streamlined approach that allows startups and small businesses to provide basic information to investors about business performance and future prospects, as well as other basic, relevant information that may be important for investor decision-making—e.g., related party transactions and conflicts of interest.

We urge the SEC to consult with the advisory committee noted above, as well as market participants and investors to develop a properly tailored approach. Consumer testing may be a useful tool as well, and the SEC should not be shy about adjusting its approach based on how they work in the marketplace.

When selling securities to the public, companies and the key players involved have a special obligation to provide truthful information. When they do not, the law properly holds them accountable. This is an essential civil right that has long been a critical tool

ensuring U.S. markets are the deepest and most reliable capital markets in the world.

Here too, the law seeks to adopt a fair, practical approach. The CROWDFUND Act sets forth a ''due diligence'' standard for accountability, which is essentially a ''do your homework'' standard. This is a standard that was reached after considerable bipartisan effort as well as consultation with legal experts, and I believe it is and can be workable and effective for this marketplace.

The promise of crowdfunding is that centralized platforms and social media can allow the ''wisdom of the crowd'' to help direct capital to deserving start-ups and small businesses in a cost-effective, efficient manner that provides fair returns. Critical to the success of the venture is the reliability of the information and commentary presented. While the Internet can be a tremendous tool for transparency, that is not always the case. The CROWDFUND Act seeks to provide a reliable, transparent marketplace by centralizing information about the offering on a registered intermediary that maintains strong standards.

Off-platform advertising is limited to pointing the public to the registered intermediary. Whether on or off the intermediary, persons paid or financially incentivized to promote—including officers, directors, and 20 percent shareholders—must clearly disclose themselves each and every time they engage in a promotional activity. Furthermore, the limitation on off-platform advertising is intended to prohibit issuers—including officers, directors, and 20 percent shareholders—from promoting or paying promoters to express opinions outside the platform that would go beyond pointing the public to the funding portal. Such paid testimonials and manufactured excitement would represent a prohibited form of off-site advertising if those disclosures were not present. Whether on or off the platform, paid advertising must clearly be disclosed as such. In short, the investor deserves a transparent medium for making healthy decisions.

These limits will help to ensure that ordinary investors can rely on the information they encounter online and accurately gauge a company's level of public support, while also helping to ensure that honest startups can compete for investors without hiring armies of paid promoters or engaging in manipulative tactics.

Another important issue the SEC will need to address is the relationship of crowdfunding to other capital raisings, and in particular to Regulation D offerings. This is a difficult issue, especially as Regulation D's restrictions on general solicitation have been loosened by Title II of the JOBS Act. I believe that careful study and attention needs to be paid to how the two should interact in various contexts, including with respect to integration.

Although crowdfunding is a public offering, it is unlike other public offerings, and, absent evidence of problems, most likely should be able to proceed parallel to a Regulation D private offering, provided the appropriate protections are put in place—and the SEC adjusts them as necessary based on their performance in the real world. It is critical, though, that the now-looser solicitation rules for a post-JOBS Act Regulation D offering not be permitted to undermine the centralized transparency protections of crowdfunding's restrictions on advertising. One solution could be to provide a safeharbor from integration rules only where the Regulation D offering followed the pre-JOBS Act approach on Regulation D. Naturally, the Regulation D offering and the crowdfunding offering would have to provide the same information to investors.

With respect to subsequent offerings, crowdfunding should be flexible enough to fit into the start-up ecosystem, and the SEC should carefully investigate this question. However, crowdfunding investors will likely face a higher risk of unfair dilution than ordinary angel investors. The disclosures mandated in the CROWDFUND Act should be helpful. But, should issuers seek to engage in private offerings within only a short period after a crowdfunding, which would normally not be permitted under Regulation D, the SEC should consider whether it can be possible for these offerings can proceed if they are especially protective of investors along the lines of how an angel investor might protect himself or herself from unfair dilution or other problems arising from near-term subsequent offerings.

This may require the SEC to adopt approaches more substantive than is normally the case. For example, dilution might only be permitted to the same or lesser extent than the directors, officers, and major shareholders, or the crowd would have to be bought out at a profit disclosed in the original offering. Again, for the success of the crowdfunding marketplace, the SEC should ensure that crowdfunding fits into the start-up ecosystem but should do so in a way that ensures crowdfunding investors are treated fairly.

Similar issues may arise with respect to other corporate governance matters and relationships with other aspects of securities law, such as managing the large number of investors in a crowdfunded company. In these instances, the SEC should look to find ways to ensure that investors are properly protected—in many instances, by ensuring that they are aligned with the interests of the directors, officers, and major shareholders—while also being practical and ensuring that crowdfunding can function within the start-up ecosystem.

Two important investor protections in the CROWDFUND Act are the public review period and withdrawl rights. They are designed to allow investors the chance to carefully consider offerings, permitting the ''wisdom of the crowd'' to develop, rather than perhaps just the ''excitement of the crowd.''

The public review period commences upon the date 21 days prior to when the securities are ''sold'' to any investor. This means that when the offering is made available to the public—''potential investors''—to consider investing: i.e., it is put up on the platform which is the point at which information is made available to regulators and is also the point when a notice filing is made with the relevant state securities regulator the public has 21 days to review it. At the end of that, the offering can close and the securities can be ''sold'' to investors. The 21-day period does not reset for each and every potential investor who might look at the offering—which is why the language specifically says ''potential investors.'' For example, when a potential investor considers investing on the seventeenth day the offering has been up on the platform, the offering can still close four days later whether that person invests or not.

The SEC must also provide appropriate ways for investors to cancel commitments to invest.

The law envisions an important role for State securities regulators. The State securities regulators are the ''50 cops on the beat'' that have time and again proven crucial for policing smaller offerings, such as those envisioned under crowdfunding.

One way the law has been designed to empower them is through the 21-day public review period for all offerings. When combined with the notice filings to the State securities regulator of the principal place of business of the issuers—and States where more than 50 percent of investors are located—and the anti-fraud authority preserved for them, the 21-day public review period is designed to provide the State securities regulators with practical ability to assist in policing the marketplace.

In addition, State securities regulators have examination and enforcement power for funding portals headquartered in their states. Although they will be limited to enforcing federal rules, this oversight authority is an important tool, especially for smaller crowdfunding portals that may emerge in particular states. Of course, oversight should be coordinated with the SEC and the relevant national securities association to the greatest extent possible.

I also encourage the SEC and the relevant national securities association to work closely with state regulators in crafting the rules and learning from their on-the-ground experience.

We have also heard recently from the CDFI community with ideas about how crowdfunding can support their work bringing growth and job creation to underserved communities. CDFIs are lenders and partners to businesses in underserved communities. They tend to obtain low rates of return on mission-driven investments, and frequently encounter financing gaps that

might be filled through mission-driven crowdfunding—much the way such investing occurs in certain segments of the non-security-based crowdfunding universe today.

I believe that the overall structure of our bill offers CDFI's powerful tools to support their job-creation work, while protecting ordinary investors from undue risk of fraud and loss. In addition, some in the CDFI community have suggested to us that because of the types of businesses CDFI's work with, the types of low returns that might be derived, and the particular financing gaps that might be filled through crowdfunding, that mission-driven, CDFI-supported crowdfunding may yield better results for investors and positive job creation for communities if the rules reflect the particular work they do. Suggestions include ensuring crowdfunding can fill the financing gap for projects supported by federally-regulated, 501(c)3 CDFIs, a clarification to ensure that CDFIs and issuers can make sure investors understand the mission and charitable aspects of investments, and fast treatment from the SEC and FINRA related to registration and membership.

The SEC should be receptive to concepts CDFIs may bring that could aid in accomplishing the job-creating goals of the legislation, while protecting investors. It should consult with CDFI's and the CDFI Fund at the Treasury Department on how best to maximize the social and jobs potential for investing through crowdfunding and CDFI's.

Although it was not included in the final legislation for procedural reasons, I would encourage the SEC and the relevant national securities association to engage in regular reviews and reports regarding developments in the crowdfunding marketplace, including thorough coordination and consultation with State securities regulators. Should problems arise, these authorities should act quickly, including use of their full rulemaking and enforcement authorities. Crowdfunding holds great potential, but it is also experimental and presents risks. For it to succeed long-term, it will require careful oversight, especially during the early stages.

I also urge the SEC and the relevant national securities association to speed the publication of final rules. Crowdfunding cannot get started until rules fill out the framework to make the law effective.

I believe the features outlined above are essential if crowdfunding is going to succeed. Success should be judged both on returns to and satisfaction of investors, and the growth and development of new and exciting companies. I am excited about the potential of this new market, but also cognizant of its risks. It won't be without its hiccups in the short run, but done properly, I believe this framework has the potential over the long run to help millions of new startups get the funding they need to grow their businesses and create jobs, and provide investors with opportunities for meaningful returns and community involvement.

I wish to extend my heartfelt thanks to the hard work and cooperation of my fellow senators, especially MICHAEL BENNET, MARY LANDRIEU, and SCOTT BROWN. I would also like to acknowledge the hard work of our staffs, who did so much to get the original legislative idea into law in strong, responsible form.

CONGRATULATING OLIVIA CULPO, MISS USA

Mr. REED. Mr. President, today I congratulate Olivia Culpo of my own hometown, Cranston, RI, for being crowned Miss USA on June 3, 2012, in Las Vegas, NV. She is the first titleholder from our State.

A native Rhode Islander, Olivia attended St. Mary Academy-Bay View and graduated with high honors. She is currently a sophomore at Boston University and has been on the dean's list every semester. Olivia is also an accomplished cellist who has performed with the Rhode Island Philharmonic Pops Orchestra, the Boston Symphony Orchestra, the Rhode Island Philharmonic Youth Orchestra, the Rhode Island Philharmonic Chamber Ensemble, the Bay View Orchestra, and the Rhode Island All-State Orchestra.

I had the pleasure of meeting Olivia recently when she came to Capitol Hill to passionately advocate for ovarian cancer prevention. Olivia is an impressive and intelligent young woman, and I appreciated the opportunity to discuss this and other issues with her.

Rhode Island is very proud that such a talented young woman is representing our State. We look forward to continuing to see Olivia serve as a positive role model both during and beyond her reign as Miss USA, and wish her the best of luck when she represents the United States at the Miss Universe pageant in December. Once again, I offer my sincerest congratulations to Olivia Culpo for being the first Rhode Islander to be crowned Miss USA.

Mr. WHITEHOUSE. Mr. President, I rise today to recognize Rhode Island native Olivia Culpo for her recent win of the Miss USA title. Miss Culpo is the first Rhode Islander to win the Miss USA competition, and my fellow Rhode Islanders and I couldn't be happier for her. We offer her our heartfelt congratulations.

A Cranston native, 20-year-old Olivia is the middle child of Peter and Susan Culpo. As a parent myself, I would especially like to extend my congratulations to Peter and Susan, who I know must be extremely proud of their daughter's accomplishment.

Olivia sets a great example for all Rhode Island children, graduating from Rhode Island's own St. Mary's Academy Bay View as a member of the National Honor Society. She currently attends Boston University in neighboring Massachusetts, where she has made the dean's list every semester.

In addition to excelling in her academic studies, Miss Culpo is a talented and dedicated musician. With two musicians for parents, Olivia was encouraged to pursue her love for music at a young age. She took cello lessons from second grade on, and has since performed with the Rhode Island Philharmonic Youth Orchestra, RI Philharmonic Chamber Ensemble, Bay View Orchestra, and Rhode Island All-State Orchestra. She has also had the distinct honor of performing with the Boston Symphony Hall in Boston and Carnegie Hall in New York City, and completed a tour of England in 2010. Most recently, Olivia performed with the Boston Accompanietta.

Olivia will spend her yearlong reign as Miss USA giving back to the community by raising awareness about breast and ovarian cancer, and by working closely with organizations fighting to find cures for these devastating diseases.

I would like to thank Miss Culpo for being a great representative for the State of Rhode Island in the Miss USA pageant, and again offer my congratulations to her and her family on her incredible win.

ADDITIONAL STATEMENTS

RECOGNIZING KATRINA COBB

● Mr. BARRASSO. Mr. President, I wish to take the opportunity to express my appreciation to Katrina Cobb for her hard work as an intern in my Casper office. I recognize her efforts and contributions to my office as well as to the State of Wyoming.

Katrina is a native of Mills, WY and a graduate of Booker High School. She currently attends the University of Wyoming where she is majoring in economics and minoring in psychology. She has demonstrated a strong work ethic which has made her an invaluable asset to our office. The quality of her work is reflected in her great efforts over the last several months.

I wish to thank Katrina for the dedication she has shown while working for me and my staff. It was a pleasure to have her as part of our team. I know she will have continued success with all of her future endeavors. I wish her all my best on her next journey.●

RECOGNIZING KELLY CURUCHET

● Mr. BARRASSO. Mr. President, I wish to take the opportunity to express my appreciation to Kelly Curuchet for her hard work as an intern for the U.S. Senate Republican Policy Committee. I recognize her efforts and contributions to my office.

Kelly is a native of Kaycee, WY, and a graduate of Kaycee High School. She recently graduated from the University of Wyoming, where she majored in business administration and minored

in professional writing. She has demonstrated a strong work ethic, which has made her an invaluable asset to the U.S. Senate Republican Policy Committee. The quality of her work is reflected in her great efforts over the last several months.

I want to thank Kelly for the dedication she has shown while working for me and my staff. It was a pleasure to have her as part of our team. I know she will have continued success with all of her future endeavors. I wish her all my best on her next journey.●

RECOGNIZING ANA KATZ

● Mr. BARRASSO. Mr. President, I wish to take the opportunity to express my appreciation to Ana Katz for her hard work as an intern in my Casper office. I recognize her efforts and contributions to my office as well as to the State of Wyoming.

Ana is a native of Casper, WY, and a graduate of Kelly Walsh High School. She currently attends the University of California, San Diego, where she is majoring in political science and history and minoring in environmental studies. She has demonstrated a strong work ethic, which has made her an invaluable asset to our office. The quality of her work is reflected in her great efforts over the last several months.

I want to thank Ana for the dedication she has shown while working for me and my staff. It was a pleasure to have her as part of our team. I know she will have continued success with all of her future endeavors. I wish her all my best on her next journey.●

RECOGNIZING KAISER MOCK

● Mr. BARRASSO. Mr. President, I wish to take the opportunity to express my appreciation to Kaiser Mock for his hard work as an intern in my Washington, D.C. office. I recognize his efforts and contributions to my office as well as to the State of Wyoming.

Kaiser is a native of Gillette, WY, and a graduate of Campbell County High School. He is a student at Michigan State University where he is majoring in Accounting. He has demonstrated a strong work ethic, which has made him an invaluable asset to our office. The quality of his work is reflected in his great efforts over the last several months.

I want to thank Kaiser for the dedication he has shown while working for me and my staff. It was a pleasure to have him as part of our team. I know he will have continued success with all of his future endeavors. I wish him all my best on his next journey.●

RECOGNIZING BEN NELSON

● Mr. BARRASSO. Mr. President, I would like to take the opportunity to express my appreciation to Ben Nelson for his hard work as an intern in my Washington, D.C. office. I recognize his efforts and contributions to my office as well as the State of Wyoming.

Ben is a native of Torrington, WY and a graduate of Torrington High School. He recently studied Interdisciplinary Studies at Eastern Wyoming College and will soon be a student at the University of Wyoming, where he will major in Political Science. He has demonstrated a strong work ethic, which has made him an invaluable asset to our office. The quality of his work is reflected in his great efforts over the last several months.

I thank Ben for the dedication he has shown while working for me and my staff. It was a pleasure to have him as part of our team. I know he will have continued success with all of his future endeavors. I wish him all my best on his next journey.●

RECOGNIZING SHAWNA PRAEUNER

● Mr. BARRASSO. Mr. President, I would like to take the opportunity to express my appreciation to Shawna Praeuner for her hard work as an intern in my Cheyenne office. I recognize her efforts and contributions to my office as well as to the State of Wyoming.

Shawna is a native of Newcastle, WY and a graduate of Newcastle High School. She recently graduated from the University of Wyoming, where she is majored in Agricultural Communications and Marketing. She has demonstrated a strong work ethic, which has made her an invaluable asset to our office. The quality of her work is reflected in her great efforts over the last several months.

I thank Shawna for the dedication she has shown while working for me and my staff. It was a pleasure to have her as part of our team. I know she will have continued success with all of her future endeavors. I wish her all my best on her next journey.●

RECOGNIZING CHARLIE ROLLINO

● Mr. BARRASSO. Mr. President, I would like to take the opportunity to express my appreciation to Charlie Rollino for his hard work as an intern for the U.S. Senate Republican Policy Committee. I recognize his efforts and contributions to my office.

Charlie is from Lander, WY and a graduate of Mother of Divine Grace High School. He is a student at Christendom College where he is majoring in History and Political Science. He has demonstrated a strong work ethic, which has made him an invaluable asset to the U.S. Senate Republican Policy Committee. The quality of his work is reflected in his great efforts over the last several months.

I thank Charlie for the dedication he has shown while working for me and my staff. It was a pleasure to have him as part of our team. I know he will have continued success with all of his future endeavors. I wish him all my best on his next journey.●

RECOGNIZING BRIANNA STRAUB

● Mr. BARRASSO. Mr. President, I would like to take the opportunity to express my appreciation to Brianna Straub for her hard work as an intern in my Sheridan office. I recognize her efforts and contributions to my office as well as to the State of Wyoming.

Brianna is a native of Kaycee, WY and a graduate of Kaycee High School. She currently attends the University of Wyoming, where she is majoring in communications. She has demonstrated a strong work ethic, which has made her an invaluable asset to our office. The quality of her work is reflected in her great efforts over the last several months.

I thank Brianna for the dedication she has shown while working for me and my staff. It was a pleasure to have her as part of our team. I know she will have continued success with all of her future endeavors. I wish her all my best on her next journey.●

RECOGNIZING THOMAS SULLIVAN

● Mr. BARRASSO. Mr. President, I would like to take the opportunity to express my appreciation to Thomas Sullivan for his hard work as an intern in my Washington, D.C. office. I recognize his efforts and contributions to my office.

Thomas is a native of Laramie, WY where he was homeschooled. He graduated from the University of Northern Colorado where he majored in business administration and accounting. He has demonstrated a strong work ethic, which has made him an invaluable asset to our office. The quality of his work is reflected in his great efforts over the last several months.

I thank Thomas for the dedication he has shown while working for me and my staff. It was a pleasure to have him as part of our team. I know he will have continued success with all of his future endeavors. I wish him all my best on his next journey.●

RECOGNIZING DAVID WISE

● Mr. BARRASSO. Mr. President, I would like to take the opportunity to express my appreciation to David Wise for his hard work as an intern in the Senate Committee on Indian Affairs. I recognize his efforts and contributions to my office as well as to the State of Wyoming.

David is a native of McLean, VA and graduated from Langley High School. He attends Clemson University where he is majoring in political science. He has demonstrated a strong work ethic, which has made him an invaluable asset to the Senate Committee on Indian Affairs. The quality of his work is reflected in his great efforts over the last several months.

I want to thank David for the dedication he has shown while working for me and my staff. It was a pleasure to have him as part of our team. I know

he will have continued success with all of his future endeavors. I wish him all my best on his next journey.●

RECOGNIZING NATALYA WOLFLEY

● Mr. BARRASSO. Mr. President, I would like to take the opportunity to express my appreciation to Natalya Wolfley for her hard work as an intern in the Senate Committee on Indian Affairs. I recognize her efforts and contributions to my office as well as to the State of Wyoming.

Natalya is a native of Etna, WY, and a graduate of Star Valley High School. She currently attends the University of Wyoming, where she is majoring in international relations and minoring in international business and Chinese. She has demonstrated a strong work ethic, which has made her an invaluable asset to the Senate Committee on Indian Affairs. The quality of her work is reflected in her great efforts over the last several months.

I want to thank Natalya for the dedication she has shown while working for me and my staff. It was a pleasure to have her as part of our team. I know she will have continued success with all of her future endeavors. I wish her all my best on her next journey.●

TRIBUTE TO MAJOR GENERAL HUGH BROOMALL

● Mr. COONS. Mr. President, it is with great pleasure that I pay tribute to MAJ General Hugh Broomall. After spending nearly 38 years serving Delaware and our Nation with the Delaware National Guard, General Broomall is retiring. He will leave behind an organization he helped to strengthen and a legacy of service that will not soon be forgotten. A native of Wilmington, DE, General Broomall's military career began when he enlisted in the Delaware Air National Guard, where he went on to receive a commission in 1974. General Broomall became an air intelligence officer and deployed worldwide in support of exercises and contingencies. Most recently, General Broomall served as the special assistant to the Director of the Air National Guard, where he was responsible for strategy development, State and Federal liaison, interagency coordination, and special studies supporting the 106,000 Air National Guard members nationwide.

General Broomall's impact is not limited to Delaware. When asked about General Broomall, LTG Bud Wyatt said, ''his multi-dimensional experience, both civilian and military, makes him an outstanding asset to the Nation. His tireless work with the military, private industry and the Hill during critical budget times, directly contributed to keeping the Air National Guard ready, relevant and reliable to serve both our state and federal military requirements well into the future. He is an outstanding American.''

I couldn't agree more. And so, I congratulate Hugh Broomall for his years of exemplary service and countless contributions to the Delaware National Guard, as well as the national military community, the people of Delaware and the country that he loves. General Broomall is an exemplary citizen, and on behalf of all Delawareans I would like to thank him and his family for their many sacrifices during his 38 years of service and wish him well in his retirement.●

TRIBUTE TO SYLVIA WOODS

● Mrs. GILLIBRAND. Mr. President, I wish to pay tribute to Sylvia Woods, the ''Queen of Soul Food'' and a New York icon whose eponymous restaurant for decades served as a home away from home for scores of Harlem residents, New Yorkers, Presidents, dignitaries, celebrities, and visitors from all over the world.

As we commemorate the 50th anniversary of Sylvia's Restaurant, we celebrate the life and legacy of Sylvia Woods. Ms. Woods' big heart, entrepreneurial spirit, and extraordinary strength exemplified the vibrancy of the Harlem community she helped bring together.

Ms. Woods was born in Hemingway, SC, in 1926. In 1954, she worked as a waitress at Johnson's Luncheonette in Harlem. Her mother helped Ms. Woods pursue her dreams by mortgaging the farm in South Carolina where Sylvia was born. Ms. Woods and her late husband Herbert used the $18,000 borrowed from her mother to buy the luncheonette in 1962 and founded the namesake restaurant.

Ms. Woods' dream became an instant reality when people from all over the world flocked to 126th Street and Lenox Avenue to taste Sylvia's world-famous comfort food, including mouthwatering fried chicken, collard greens, and peach cobbler. Ms. Woods purchased six lots which took up nearly one city block on Lenox Avenue between 126th and 127th Streets, setting in motion the growth of the legendary soul food establishment. She ran the business until she retired at age 80 and had overseen its expansion to seat more than 450 people.

Her famed eatery not only became a center of globally-renowned cuisine, but it also became a special meeting place for African-American leaders. I fondly remember Sylvia's being one of the first places I visited with Rev. Al Sharpton in 2009 as Senator. I, along with countless others, deeply felt the love, life, and history of this iconic institution.

Ms. Woods cared deeply about the community she loved and found ways to give back to her beloved Harlem. The Woods family created the Sylvia and Herbert Woods Scholarship Endowment Foundation in 2001 to provide scholarships to Harlem youth.

Ms. Woods undoubtedly made an indelible impact on our great city and Nation. The landmark restaurant she created will continue to thrive for future generations of New York City families. Ms. Woods' legacy, accomplishments, and endearing spirit will live on in Harlem and around the world.●

TRIBUTE TO THE DISABILITY RIGHTS MOVEMENT

● Mr. HARKIN. Mr. President, the National Constitution Center in Philadelphia, which opened on July 4, 2003, is the first and only nonprofit, nonpartisan institution devoted to the world's oldest and most respected framework for democratic government: the Constitution of the United States. Located on historic Independence Mall, the center is many things: an interactive museum, a national town hall, and a civic hub for millions of visitors from around the world. It inspires active citizenship by shining a spotlight on our great constitutional principles, ideals, and freedoms.

This Saturday, the center's main exhibition, which is called ''The Story of We the People,'' is inaugurating an important new addition: the wheelchair used by disability-rights advocate Justin Dart, Jr., when he was present alongside President George H.W. Bush at the signing of the Americans with Disabilities Act on July 26, 1990. Mr. Dart used that wheelchair on countless other occasions as he advocated for passage of the Americans with Disabilities Act and to secure for people with disabilities the civil rights that all Americans hold sacred.

This wonderful new addition to the National Constitution Center will serve as a symbol of freedom for all Americans. The wheelchair will remind visitors of the visionary leadership and inspired advocacy of Justin Dart, Jr., and the courageous struggle of all those in the disability rights movement who fought to pass the ADA, one of the great civil rights laws of the 20th century, often referred to as the Emancipation Proclamation for people with disabilities.

Twenty-two years ago today, as President Bush signed the ADA into law, he said: ''Let the shameful wall of exclusion finally come tumbling down.'' I was present at that White House ceremony, and I vividly remember the joy and pride on Justin Dart's face as he sat aside the President. As of this Saturday, visitors to the National Constitution Center, when they view Justin Dart's wheelchair and accompanying photos, will be able to relive that great moment and milestone in our Nation's history.●

CONGRATULATING CLARISSA MARTINS

● Mr. HELLER. Mr. President, today I wish to congratulate one of Nevada's own, Clarissa Martins. Clarissa is a student at the University of Nevada, Reno, who was recently awarded the 2012 Thomas J. Bardos Award for her participation in cancer and nutrition

research. Presented by the American Association of Cancer Research, this prestigious award recognizes and encourages young science students to pursue the field of cancer research. I am proud to honor Clarissa for her commitment to the scientific community in addressing a deadly disease that affects thousands of Nevadans each year.

For UNR senior, Clarissa, the devastating impact of cancer hit home when her mother lost her battle with pancreatic cancer in 2009. Inspired by her mother, Clarissa began researching the intricacies of this fatal disease. She is currently working on a UNR research project to determine rates of breast and lung cancer.

As someone whose family has been touched by cancer, I am humbled by Clarissa's efforts to study the second most common cause of death in America. Cancer is one of our most pressing health concerns in this country. Over 1.6 million new cancer cases will be diagnosed this year, and more than half a million Americans will lose their lives to this disease. In order for our country to be better prepared to combat this devastating disease, we must continue to research and provide better oncology care.

I am proud that such an ambitious student calls Nevada home, and that she has remained committed to fighting this deadly disease. I wish Clarissa continued success and the best of luck in her future academic endeavors. Today, I ask my colleagues to join me in congratulating her on this great accomplishment.●

2012 OLYMPIC GAMES

● Mr. INHOFE. Mr. President, this Friday marks the beginning of the 2012 London Olympic Games. Every 4 years, our national pride is displayed as we join our family and friends to cheer on Team USA. In this summer's London Games, the 530-member U.S. team will compete in 25 sports that span 246 medal events. Individuals and families make so many sacrifices just to have the opportunity to be a part of these competitions every 4 years. Rigorous physical challenges, early morning workouts, and total commitment are hallmarks of Olympians. Support of family and friends are also key to the success of these athletes.

Several of the team members have ties to my home State of Oklahoma. Many basketball players have Oklahoma ties—Blake Griffin, James Harden, Kevin Durant, and Russell Westbrook are all members of the USA basketball team. Many of us have followed Griffin's career from his early days, even before he was a University of Oklahoma Sooner. Then, of course Durant, Westbrook, and Harden are members of the Oklahoma City Thunder team that captivated our State and drew us together on their amazing journey through the NBA playoffs this past season.

All eyes will be on the Team USA's rowing team as they compete for a medal. Anthony Fahden of Oklahoma City, Will Newell of Oklahoma City, Tom Peszek of Oklahoma City, Nick LaCava of Oklahoma City, and Robin Prendes of Oklahoma City, will compete in rowing events.

Our State has a rich wrestling heritage. Three wrestlers, one from Oklahoma State University and two from the University of Oklahoma, will represent our Nation and State. Cowboy Coleman Scott and Sooners Jared Frayer and Sam Hazewinkel will continue that tradition in London as they hit the mat for Team USA.

Oklahoma will also be represented during the track and field events. Tia Brooks, a shot putter residing in Norman, secured a spot on the Olympic team with a big second throw at the U.S. trials. Brittany Borman, a javelin thrower also residing in Norman, secured first place and a spot on the U.S. team on her final throw at U.S. trials.

In gymnastics, Norman resident Jake Dalton will regale audiences on the vault and floor exercises. Meanwhile, in the pool, Mary Killman, who was born in Ada, will compete in solo, duet, and team synchronized swimming.

My wife Kay and I and our 20 kids and grandchildren will be watching these individuals and the entire U.S. Olympic team during the London Games, and we wish them every success as they make our State and our entire Nation proud.●

MOUNTAIN STATE SECURITY FELLOWSHIP

● Mr. MANCHIN. Mr. President, I rise today to recognize the thousands of West Virginians who have chosen to serve this great Nation as members of our military. West Virginia is one of the most patriotic States in the Nation, and we are humbled by the sacrifice of 39 brave West Virginians who gave their lives in Iraq and Afghanistan.

Throughout the generations, thousands of brave men and women gave us our freedom; they deserve the best we can give them in return.

In recognition of these values and the service of all West Virginians, today I am launching the Mountain State National Security Fellowship.

While working on Capitol Hill or in my State offices, selected fellows will use the skills and experience gained while serving in our armed services to assist my office with military and veterans-related issues. They will also personally represent the West Virginia veteran community and embody the values of all who served, including those who made the ultimate sacrifice for their country.

This is our next generation of leaders, and this fellowship will help encourage them to develop their interest in public service. Fellows will gain a firsthand understanding of how we help our constituents by staying connected to their lives and serving their needs. Our office will benefit from a servicemember's perspective on the problems we are trying to solve.

This fellowship is a small but important step in a much larger national problem. Veterans face the highest unemployment levels of almost any group of people in our economy, and that is wrong. We need to do more to match our veterans with available jobs in their communities.

As cofounder of the Congressional Veterans Jobs Caucus, I have joined with many colleagues from both parties to focus on the problem of veterans' unemployment. As we draw down from the Middle East, veterans will be returning to our communities and trying to build new lives with their families, and we should do everything we can to put their incredible skills to good use.

In my own office, we employ four veterans, and they are the most dedicated, trained, committed kind of employees imaginable. I am so appreciative to have that quality of a workforce in my office.

As a nation, we fly the flag and we proudly display yellow ribbons, but if you really want to say thank you to someone who was willing to sacrifice and give their all, you hire a veteran. They are well trained, disciplined, and ready to go to work.

That is the drive behind our jobs caucus, our ''I Hire Veterans'' project, and this fellowship program. It is easy to talk the talk, but you have to walk the walk, and this fellowship is one way for us to do so.

I want to say thank you to all West Virginia veterans and their families and that it will be an honor to work with you as Mountain State National Security Fellows.●

RECOGNIZING COZY HARBOR SEAFOOD

● Ms. SNOWE. Mr. President, with over 220 miles of beautiful Atlantic coastline, my home State knows the benefits and the rigors of living off the water. The very mention of Maine will evoke, for many, the pristine natural beauty and rugged terrain of our rocky coast. Hand in hand with these romantic images is that of hard-working fishermen, whose relationship with Maine's waters is key to maintaining a thriving seafood market so characteristic of our State. I rise to recognize a small business whose dedication to producing and marketing a quality product epitomizes the entrepreneurial spirit so characteristic of Maine.

From its founding in 1980, Cozy Harbor Seafood of Portland, ME has striven to provide a consistently high-quality product to consumers both local and abroad with a recent expansion into the European markets. Specializing in processing and distributing lobster, fresh fish, and frozen seafood for supermarkets, seafood wholesalers,

and restaurants, Cozy Harbor is aggressively seeking new venues and opportunities to expand through participation in seafood expositions, as seen through its recent involvement at the European Seafood Exposition and the upcoming Asian Seafood Show and China Fisheries Show later this year.

The seafood industry in Maine is more than a profession; it is a lifestyle. The passion, love, and dedication shown by those in my home State to producing a quality product not only reaps its benefits in the ledger books, it is also a major contributing factor in the development of the tradition and reputation of excellence that Maine seafood has come to be known for worldwide. Through programs such as the Gulf of Maine Responsibly Harvested Program, the sustainability of the fishing industry is further developed. Cozy Harbor also participates in the Trace Register which records the product's origin for consumers to view online, has been recognized internationally for high-quality product, and has received the British Retail Consortium's certification grade A level for food safety. These efforts not only increase quality standards, they ensure that the fishing industry is viable for generations to come.

Like many small businesses in Maine, Cozy Harbor is steadfast in serving the local community and giving back to the area. Its devotion is illustrated by its donation of approximately 500 lobsters to the Bike MS: Great Maine Getaway sponsored annually by the National MS Society's New England chapter, which supports multiple sclerosis research and programs in the New England area.

Cozy Harbor exhibits the ingenuity, commitment to quality, and dedication to competing in an ever-growing market that is so characteristic of entrepreneurs in Maine. I commend Cozy Harbor on its success and offer my best wishes for the future.●

TRIBUTE TO ARVID ''BUTCH'' HILLER

● Mr. TESTER. Mr. President, I rise to honor a fellow Montanan today as he retires from a long and distinguished career in the water utility business after 41 years. Arvid ''Butch'' Hiller retires from the Mountain Water Company in Missoula, where he is the general manager.

Butch Hiller was raised in Missoula. He spent 10 years supplying water to his community through Montana Power and 32 years when it became the Mountain Water Company. In other words, Mountain Water has never run a day without Butch Hiller contributing to its mission. His distinguished career at Mountain Water included recognition by his profession, including the Distinguished Public Service Award from the American Water Works Association in 2005. His contributions to the Missoula community and the State of Montana are numerous, including service on the Missoula Rotary Club, the Missoula and the Montana Chambers of Commerce, the Montana Power Business Information Panel, and the Montana Ambassadors.

Butch has said one of the keys to his success has been to hire people who were better and smarter to help him do what he alone could not do. He also said he tried to give people the freedom to achieve success and to learn from their mistakes.

Mr. President, water is our most basic resource. Butch Hiller spent a career as a caretaker of that precious resource. As he and his wife Lynn begin their retirement and continue to enjoy their four children and five grandchildren, I would like to join with other Montana residents and thank Butch for his stewardship of our Montana water and the many contributions he has made to our community.●

OAHE DAM

● Mr. THUNE. Mr. President, today I wish to recognize the 50th anniversary of construction of the Oahe Dam.

In December 1944, President Franklin D. Roosevelt approved the Flood Control Act. This set into motion the construction of several dams across South Dakota. Construction on the Oahe Dam commenced in 1948 and was completed in 1962. In August of 1962, President John F. Kennedy dedicated the dam located in central South Dakota on the Missouri River. The dam was a massive endeavor for the U.S. Army Corps of Engineers, standing 245 feet tall with an earth fill volume of 92 million cubic yards and a concrete fill volume of 1,122,000 yards. The reservoir stretches 231 miles to Bismarck, ND. The Oahe Dam is the 14th largest manmade reservoir in the world.

Oahe Dam is beneficial not only to South Dakota but throughout the Midwest. The powerplant on the dam is the largest producer of energy on the Missouri River. North Dakota, South Dakota, Nebraska, Minnesota, and Montana receive power produced by the Oahe Dam. Local farmers and ranchers benefit from the irrigation that is provided from the reservoir.

I would like to recognize the efforts of all those who have contributed to the construction and maintenance of the Oahe Dam. It has become one of South Dakota's greatest resources.●

RECOGNIZING GROSSENBURG IMPLEMENT

● Mr. THUNE. Mr. President, today I wish to recognize the 75th anniversary of Grossenburg Implement. The company was founded during the Great Depression in 1937 by Charles Jacob Grossenburg in Tripp County, SD. The demand for two-cylinder tractors during World War II led to the company's success and prosperity. Since then, Grossenburg Implement has stayed true to their mission statement ''to provide the best product at a reasonable price and with the highest level of service.'' Along with products from John Deere, Grossenburg sold Oldsmobile and Cadillac automobiles. Throughout the years, the Grossenburg family remained dedicated to quality service and continued success.

Charlie, son of Barry and Marilyn Grossenburg, represents the fourth generation of the family business and is now the vice president. In 1998, Grossenburg Implement continued its success by adding a combine shop in Winner and subsequently an overhead crane to the shop in 2005. In 2009, the company also celebrated the opening of another combine shop in Pierre. Most recently in 2012, the company expanded their business by purchasing Northeast Equipment, Inc. in Nebraska. Today, the company has grown from one store to a projected $150 million company.

I would like to congratulate the Grossenburg family and the employees of Grossenburg Implement for 75 years of success and wish them a prosperous future.●

MESSAGES FROM THE HOUSE

ENROLLED BILL SIGNED

The President pro tempore (Mr. INOUYE) announced that on today, July 26, 2012, he had signed the following enrolled bill, previously signed by the Speaker of the House:

S. 1335. An act to amend title 49, United States Code, to provide rights for pilots, and for other purposes.

At 1:32 p.m., a message from the House of Representatives, delivered by Mrs. Cole, one of its reading clerks, announced that the House has passed the following bills, in which it requests the concurrence of the Senate:

H.R. 459. An act to require a full audit of the Board of Governors of the Federal Reserve System and the Federal reserve banks by the Comptroller General of the United States, and for other purposes.

H.R. 6082. An act to officially replace, within the 60-day Congressional review period under the Outer Continental Shelf Lands Act, President Obama's Proposed Final Outer Continental Shelf Oil & Gas Leasing Program (2012–2017) with a congressional plan that will conduct additional oil and natural gas lease sales to promote offshore energy development, job creation, and increased domestic energy production to ensure a more secure energy future in the United States, and for other purposes.

At 6:04 p.m., a message from the House of Representatives, delivered by Mrs. Cole, one of its reading clerks, announced that the House has agreed to the following concurrent resolution, in which it requests the concurrence of the Senate:

H. Con. Res. 134. Concurrent resolution condemning, in the strongest possible terms, the heinous atrocities that occurred in Aurora, Colorado.

ENROLLED BILL SIGNED

The message further announced that the Speaker has signed the following enrolled bill:

H.R. 5872. An act to require the President to provide a report detailing the sequester

required by the Budget Control Act of 2011 on January 2, 2013.

The enrolled bill was subsequently signed by the President pro tempore (Mr. INOUYE).

MEASURES READ THE FIRST TIME

The following bill was read the first time:

H.R. 6082. An act to officially replace, within the 60-day Congressional review period under the Outer Continental Shelf Lands Act, President Obama's Proposed Final Outer Continental Shelf Oil & Gas Leasing Program (2012–2017) with a Congressional plan that will conduct additional oil and natural gas lease sales to promote offshore energy development, job creation, and increased domestic energy production to ensure a more secure energy future in the United States, and for other purposes.

ENROLLED BILL PRESENTED

The Secretary of the Senate announced that on today, July 26, 2012, she had presented to the President of the United States the following enrolled bill:

S. 1335. An act to amend title 49, United States Code, to provide rights for pilots, and for other purposes.

EXECUTIVE AND OTHER COMMUNICATIONS

The following communications were laid before the Senate, together with accompanying papers, reports, and documents, and were referred as indicated:

EC–6935. A communication from the Director of the Regulatory Management Division, Environmental Protection Agency, transmitting, pursuant to law, the report of a rule entitled ''Significant New Use Rules on Certain Chemical Substances'' (FRL No. 9354–2) received in the Office of the President of the Senate on July 19, 2012; to the Committee on Environment and Public Works.

EC–6936. A communication from the Director of the Regulatory Management Division, Environmental Protection Agency, transmitting, pursuant to law, the report of a rule entitled ''Significant New Use Rules on a Certain Chemical Substance; Removal of Significant New Use Rules'' (FRL No. 9356–1) received in the Office of the President of the Senate on July 19, 2012; to the Committee on Environment and Public Works.

EC–6937. A communication from the Director of the Regulatory Management Division, Environmental Protection Agency, transmitting, pursuant to law, the report of a rule entitled ''Approval and Promulgation of Air Quality Implementation Plans; Virginia; Removal of Administrative Requirements from the Regulation for the Control of Motor Vehicle Emissions in Northern Virginia'' (FRL No. 9702–4) received in the Office of the President of the Senate on July 19, 2012; to the Committee on Environment and Public Works.

EC–6938. A communication from the Director of the Regulatory Management Division, Environmental Protection Agency, transmitting, pursuant to law, the report of a rule entitled ''Approval and Promulgation of Implementation Plans and Designation of Areas for Air Quality Planning Purposes; Wisconsin; Redesignation of the Milwaukee-Racine Area to Attainment for 1997 8-hour Ozone Standard'' (FRL No. 9702–9) received in the Office of the President of the Senate on July 19, 2012; to the Committee on Environment and Public Works.

EC–6939. A communication from the Director of the Regulatory Management Division, Environmental Protection Agency, transmitting, pursuant to law, the report of a rule entitled ''Approval and Promulgation of Air Quality Implementation Plans; Maryland; Offset Lithographic Printing and Letterpress Printing Regulations'' (FRL No. 9702–2) received in the Office of the President of the Senate on July 19, 2012; to the Committee on Environment and Public Works.

EC–6940. A communication from the Director of the Regulatory Management Division, Environmental Protection Agency, transmitting, pursuant to law, the report of a rule entitled ''Approval and Promulgation of Implementation Plans; Tennessee; 110(a) (1) and (2) Infrastructure Requirements for the 1997 8-Hour Ozone National Ambient Air Quality Standards'' (FRL No. 9699–5) received in the Office of the President of the Senate on July 19, 2012; to the Committee on Environment and Public Works.

EC–6941. A communication from the Director, Office of Congressional Affairs, Nuclear Regulatory Agency, transmitting, pursuant to law, the report of a rule entitled ''Receipts-Based, Small Business Size Standard'' (RIN3150–AJ14) received in the Office of the President of the Senate on July 18, 2012; to the Committee on Environment and Public Works.

EC–6942. A communication from the Assistant Secretary of the Army (Civil Works), transmitting, pursuant to law, a report relative to the C–111 Spreader Canal Western project in Miami-Dade County, Florida; to the Committee on Environment and Public Works.

EC–6943. A communication from the Director of Congressional Affairs, Nuclear Regulatory Commission, transmitting, pursuant to law, the report of a rule entitled ''Technical Corrections'' (RIN3150–AJ16) received in the Office of the President of the Senate on July 18, 2012; to the Committee on Environment and Public Works.

EC–6944. A communication from the Director of Congressional Affairs, Nuclear Regulatory Commission, transmitting, pursuant to law, the report of a rule entitled ''Communication with Transport Vehicles'' (Regulatory Guide 5.32) received in the Office of the President of the Senate on July 18, 2012; to the Committee on Environment and Public Works.

EC–6945. A communication from the Director of Congressional Affairs, Nuclear Regulatory Commission, transmitting, pursuant to law, the report of a rule entitled ''Issuing Final Guidance That Issues a New Branch Technical Position BTP 8–8—(Emergency Diesel Generators) and Off Site Power Sources Allowed Outage Time Extensions'' (Publication of Revision 4 to SRP Section 8.1) received in the Office of the President of the Senate on July 18, 2012; to the Committee on Environment and Public Works.

EC–6946. A communication from the Chief of the Publications and Regulations Branch, Internal Revenue Service, Department of the Treasury, transmitting, pursuant to law, the report of a rule entitled ''Regulations Under Section 367(d) applicable to certain outbound asset reorganizations'' (Notice 2012–39) received in the Office of the President of the Senate on July 19, 2012; to the Committee on Finance.

EC–6947. A communication from the Chief of the Publications and Regulations Branch, Internal Revenue Service, Department of the Treasury, transmitting, pursuant to law, the report of a rule entitled ''Tribal Economic Development Bonds'' (Notice 2012–48) received in the Office of the President of the Senate on July 19, 2012; to the Committee on Finance.

EC–6948. A communication from the Assistant Secretary, Bureau of Legislative Affairs, Department of State, transmitting, pursuant to law, the semiannual report on the continued compliance of Azerbaijan, Kazakhstan, Moldova, the Russian Federation, Tajikistan, and Uzbekistan with the 1974 Trade Act's freedom of emigration provisions, as required under the Jackson-Vanik Amendment; to the Committee on Finance.

EC–6949. A communication from the Chairman of the United States International Trade Commission, transmitting, pursuant to law, a report entitled ''The Year in Trade 2011''; to the Committee on Finance.

EC–6950. A communication from the Assistant Secretary, Legislative Affairs, Department of State, transmitting, notice of proposed permanent transfer of significant military equipment pursuant to section 3(d) of the Arms Export Control Act (Transmittal No. RSAT–12–2990); to the Committee on Foreign Relations.

EC–6951. A communication from the Assistant Secretary, Legislative Affairs, Department of State, transmitting, notice of proposed permanent transfer of significant military equipment pursuant to section 3(d) of the Arms Export Control Act (Transmittal No. RSAT–12–2917); to the Committee on Foreign Relations.

EC–6952. A communication from the Assistant Secretary, Legislative Affairs, Department of State, transmitting, certification of proposed issuance of an export license pursuant to section 36(c) of the Arms Export Control Act (Transmittal No. DDTC 12–080); to the Committee on Foreign Relations.

EC–6953. A communication from the Assistant Secretary, Legislative Affairs, Department of State, transmitting, certification of proposed issuance of an export license pursuant to section 36(c) of the Arms Export Control Act (Transmittal No. DDTC 12–084); to the Committee on Foreign Relations.

EC–6954. A communication from the Assistant Secretary, Legislative Affairs, Department of State, transmitting, certification of proposed issuance of an export license pursuant to section 36(c) of the Arms Export Control Act (Transmittal No. DDTC 12–078); to the Committee on Foreign Relations.

EC–6955. A communication from the Assistant Secretary, Legislative Affairs, Department of State, transmitting, certification of proposed issuance of an export license pursuant to section 36(c) of the Arms Export Control Act (Transmittal No. DDTC 12–038); to the Committee on Foreign Relations.

EC–6956. A communication from the Assistant Secretary, Legislative Affairs, Department of State, transmitting, certification of proposed issuance of an export license pursuant to section 36(c) of the Arms Export Control Act (Transmittal No. DDTC 12–048); to the Committee on Foreign Relations.

EC–6957. A communication from the Assistant Secretary, Legislative Affairs, Department of State, transmitting, certification of proposed issuance of an export license pursuant to section 36(c) of the Arms Export Control Act (Transmittal No. DDTC 12–086); to the Committee on Foreign Relations.

EC–6958. A communication from the Assistant Secretary, Legislative Affairs, Department of State, transmitting, certification of proposed issuance of an export license pursuant to section 36(c) of the Arms Export Control Act (Transmittal No. DDTC 12–049); to the Committee on Foreign Relations.

EC–6959. A communication from the Assistant Secretary, Legislative Affairs, Department of State, transmitting, certification of proposed issuance of an export license pursuant to section 36(d) of the Arms Export Control Act (Transmittal No. DDTC 12–068); to the Committee on Foreign Relations.

EC–6960. A communication from the Assistant Secretary, Legislative Affairs, Department of State, transmitting, certification of proposed issuance of an export license pursuant to section 36(c) of the Arms Export Control Act (Transmittal No. DDTC 12–065); to the Committee on Foreign Relations.

EC–6961. A communication from the Deputy Director of Regulations and Policy Management Staff, Food and Drug Administration, Department of Health and Human Services, transmitting, pursuant to law, the report of a rule entitled ''Indirect Food Additives: Polymers'' (Docket No. FDA–2012–F–0031) received during adjournment of the Senate in the Office of the President of the Senate on July 20, 2012; to the Committee on Health, Education, Labor, and Pensions.

EC–6962. A communication from the Senior Procurement Executive/Deputy Chief Acquisition Officer, Office of Acquisition Policy, General Services Administration, transmitting, pursuant to law, the report of a rule entitled ''Federal Acquisition Regulation; Small Entity Compliance Guide'' (FAC 2005–60) received in the Office of the President of the Senate on July 24, 2012; to the Committee on Homeland Security and Governmental Affairs.

EC–6963. A communication from the Senior Procurement Executive/Deputy Chief Acquisition Officer, Office of Acquisition Policy, General Services Administration, transmitting, pursuant to law, the report of a rule entitled ''Federal Acquisition Regulation; Introduction'' (FAC 2005–60) received in the Office of the President of the Senate on July 24, 2012; to the Committee on Homeland Security and Governmental Affairs.

EC–6964. A communication from the Senior Procurement Executive/Deputy Chief Acquisition Officer, Office of Acquisition Policy, General Services Administration, transmitting, pursuant to law, the report of a rule entitled ''Federal Acquisition Regulation; Technical Amendments'' (FAC 2005–60) received in the Office of the President of the Senate on July 24, 2012; to the Committee on Homeland Security and Governmental Affairs.

EC–6965. A communication from the Senior Procurement Executive/Deputy Chief Acquisition Officer, Office of Acquisition Policy, General Services Administration, transmitting, pursuant to law, the report of a rule entitled ''Federal Acquisition Regulation; DARPA-New Mexico Tax Agreement'' ((RIN9000–AM290) (FAC 2005–60)) received in the Office of the President of the Senate on July 24, 2012; to the Committee on Homeland Security and Governmental Affairs.

EC–6966. A communication from the Senior Procurement Executive/Deputy Chief Acquisition Officer, Office of Acquisition Policy, General Services Administration, transmitting, pursuant to law, the report of a rule entitled ''Federal Acquisition Regulation; Clarification of Standards for Computer Generation of Forms'' ((RIN9000–AM15) (FAC 2005–60)) received in the Office of the President of the Senate on July 24, 2012; to the Committee on Homeland Security and Governmental Affairs.

EC–6967. A communication from the Senior Procurement Executive/Deputy Chief Acquisition Officer, Office of Acquisition Policy, General Services Administration, transmitting, pursuant to law, the report of a rule entitled ''Federal Acquisition Regulation; Extension of Sunset Date for Protests of Task and Delivery Orders'' ((RIN9000–AM26) (FAC 2005–60)) received in the Office of the President of the Senate on July 24, 2012; to the Committee on Homeland Security and Governmental Affairs.

EC–6968. A communication from the Senior Procurement Executive/Deputy Chief Acquisition Officer, Office of Acquisition Policy, General Services Administration, transmitting, pursuant to law, the report of a rule entitled ''Federal Acquisition Regulation; Payments Under Time-and-Materials and Labor-Hour Contracts'' ((RIN9000–AM01) (FAC 2005–60)) received in the Office of the President of the Senate on July 24, 2012; to the Committee on Homeland Security and Governmental Affairs.

EC–6969. A communication from the Senior Procurement Executive/Deputy Chief Acquisition Officer, Office of Acquisition Policy, General Services Administration, transmitting, pursuant to law, the report of a rule entitled ''Federal Acquisition Regulation; Reporting Executive Compensation and First-Tier Subcontract Awards'' ((RIN9000–AL66) (FAC 2005–60)) received in the Office of the President of the Senate on July 24, 2012; to the Committee on Homeland Security and Governmental Affairs.

EC–6970. A communication from the Presiding Governor of the Broadcasting Board of Governors, transmitting, pursuant to law, the Office of Inspector General's Semiannual Report for the period of October 1, 2011 through March 31, 2012; to the Committee on Homeland Security and Governmental Affairs.

EC–6971. A communication from the Executive Director, United States Access Board, transmitting, pursuant to law, the Board's annual report relative to the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002; to the Committee on Homeland Security and Governmental Affairs.

EC–6972. A communication from the Acting Assistant Attorney General, Office of Legislative Affairs, Department of Justice, transmitting, pursuant to law, the Department of Justice's fiscal year 2011 annual report relative to the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002; to the Committee on Homeland Security and Governmental Affairs.

EC–6973. A communication from the Director, Office of Diversity Management and Equal Opportunity, Office of the Under Secretary of Defense (Personnel and Readiness), transmitting, pursuant to law, a compilation of fiscal year 2012 reports from the Department of Defense Components relative to the implementation of the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002; to the Committee on Homeland Security and Governmental Affairs.

EC–6974. A communication from the Chairman of the National Transportation Safety Board, transmitting, pursuant to law, a report relative to the activities performed by the agency that are not inherently governmental functions; to the Committee on Homeland Security and Governmental Affairs.

EC–6975. A communication from the Chairman of the Board of Governors, U.S. Postal Service, transmitting, pursuant to law, the Office of Inspector General's Semiannual Report and the Postal Service management response to the report for the period of October 1, 2011 through March 31, 2012; to the Committee on Homeland Security and Governmental Affairs.

EC–6976. A communication from the Acting Chairman of the Federal Deposit Insurance Corporation, transmitting, pursuant to law, the Federal Deposit Insurance Corporation's 2012 Annual Performance Plan; to the Committee on Homeland Security and Governmental Affairs.

EC–6977. A communication from the District of Columbia Auditor, transmitting, pursuant to law, a report entitled, ''Sufficiency Certification for the Washington Convention and Sports Authority's (Trading as Events DC) Projected Revenues and Excess Reserve to Meet Projected Operating and Debt Service Expenditures and Reserve Requirements for Fiscal Year 2013''; to the Committee on Homeland Security and Governmental Affairs.

EC–6978. A communication from the Assistant Secretary, Bureau of Legislative Affairs, Department of State, transmitting, pursuant to law, the Department's Fiscal Year 2011 annual report relative to the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002; to the Committee on Homeland Security and Governmental Affairs.

EC–6979. A communication from the Clerk of Court, United States Court of Appeals for the Seventh Circuit, transmitting an opinion of the United States Court of Appeals for the Seventh Circuit; to the Committee on the Judiciary.

EC–6980. A communication from the Assistant Attorney General, Office of Legislative Affairs, Department of Justice, transmitting, pursuant to law, an annual report of the Review Panel on Prison Rape; to the Committee on the Judiciary.

EC–6981. A communication from the Federal Liaison Officer, Patent and Trademark Office, Department of Commerce, transmitting, pursuant to law, the report of a rule entitled ''Rules of Practice for Trials before the Patent Trial and Appeal Board and Judicial Review of Patent Trial and Appeal Board Decisions'' (RIN0651–AC70) received in the Office of the President of the Senate on July 23, 2012; to the Committee on the Judiciary.

EC–6982. A communication from the Federal Liaison Officer, Patent and Trademark Office, Department of Commerce, transmitting, pursuant to law, the report of a rule entitled ''Changes to Implement the Inventor's Oath or Declaration Provisions of the Leahy-Smith America Invents Act'' (RIN0651–AC68) received in the Office of the President of the Senate on July 23, 2012; to the Committee on the Judiciary.

EC–6983. A communication from the Federal Liaison Officer, Patent and Trademark Office, Department of Commerce, transmitting, pursuant to law, the report of a rule entitled ''Transitional Program for Covered Business Method Patents—Definitions of Covered Business Method Patent and Technological Invention'' (RIN0651–AC75) received in the Office of the President of the Senate on July 23, 2012; to the Committee on the Judiciary.

EC–6984. A communication from the Federal Liaison Officer, Patent and Trademark Office, Department of Commerce, transmitting, pursuant to law, the report of a rule entitled ''Changes to Implement the Supplemental Examination Provisions of the Leahy-Smith America Invents Act and to Revise Reexamination Fees'' (RIN0651–AC69) received in the Office of the President of the Senate on July 23, 2012; to the Committee on the Judiciary.

EC–6985. A communication from the Federal Liaison Officer, Patent and Trademark Office, Department of Commerce, transmitting, pursuant to law, the report of a rule entitled ''Changes to Implement Inter Partes Review Proceedings, Post-Grant Review Proceedings, and Transitional Program for Covered Business Methods Patents'' (RIN0651–AC71) received in the Office of the President of the Senate on July 23, 2012; to the Committee on the Judiciary.

EC–6986. A communication from the Librarian of Congress, transmitting, pursuant to law, the annual report on the activities of the Library of Congress for fiscal year 2011; to the Committee on Rules and Administration.

EC–6987. A communication from the Deputy General Counsel, Office of Financial Assistance, Small Business Administration,

transmitting, pursuant to law, the report of a rule entitled ''7(a) Loan Program; Eligible Passive Companies'' (RIN3245–AG48) received in the Office of the President of the Senate on July 24, 2012; to the Committee on Small Business and Entrepreneurship.

EC–6988. A communication from the Deputy General Counsel, Office of Investment and Innovation, Small Business Administration, transmitting, pursuant to law, the report of a rule entitled ''Small Business Investment Companies—Early Stage SBICs'' (RIN3245–AG32) received in the Office of the President of the Senate on July 18, 2012; to the Committee on Small Business and Entrepreneurship.

EC–6989. A communication from the Deputy General Counsel, Office of Investment and Innovation, Small Business Administration, transmitting, pursuant to law, the report of a rule entitled ''Small Business Investment Companies—Energy Saving Qualified Investments'' (RIN3245–AF86) received in the Office of the President of the Senate on July 18, 2012; to the Committee on Small Business and Entrepreneurship.

EC–6990. A communication from the Deputy General Counsel, Office of Investment and Innovation, Small Business Administration, transmitting, pursuant to law, the report of a rule entitled ''Small Business Investment Companies—Conflicts of Interest and Investment of Idle Funds'' (RIN3245–AF56) received in the Office of the President of the Senate on July 18, 2012; to the Committee on Small Business and Entrepreneurship.

EC–6991. A communication from the Director of the Regulatory Management Division, Environmental Protection Agency, transmitting, pursuant to law, the report of a rule entitled ''Titanium Dioxide; Exemption from the Requirement of a Tolerance'' (FRL No. 9354–6) received in the Office of the President of the Senate on July 25, 2012; to the Committee on Agriculture, Nutrition, and Forestry.

EC–6992. A communication from the Director of the Regulatory Management Division, Environmental Protection Agency, transmitting, pursuant to law, the report of a rule entitled ''Pyrimethanil; Pesticide Tolerances'' (FRL No. 9354–7) received in the Office of the President of the Senate on July 25, 2012; to the Committee on Agriculture, Nutrition, and Forestry.

EC–6993. A communication from the Director of the Regulatory Management Division, Environmental Protection Agency, transmitting, pursuant to law, the report of a rule entitled ''Acetamiprid; Pesticide Tolerances'' (FRL No. 9352–8) received in the Office of the President of the Senate on July 25, 2012; to the Committee on Agriculture, Nutrition, and Forestry.

EC–6994. A communication from the Secretary of Transportation, transmitting, pursuant to law, a report relative to a violation of the Antideficiency Act that occurred in the Maritime Administration's (MARAD) Operations and Training account (69 1750); to the Committee on Appropriations.

EC–6995. A communication from the Principal Deputy Under Secretary of Defense (Personnel and Readiness), transmitting the report of four (4) officers authorized to wear the insignia of the grade of rear admiral and rear admiral (lower half) as indicated, in accordance with title 10, United States Code, section 777; to the Committee on Armed Services.

EC–6996. A communication from the Attorney, Office of the General Counsel, Bureau of Consumer Financial Protection, transmitting, pursuant to law, the report of a rule entitled ''Defining Larger Participants of the Consumer Reporting Market'' ((RIN3170–AA00) (Docket No. CFPB–2012–0005)) received in the Office of the President of the Senate on July 25, 2012; to the Committee on Banking, Housing, and Urban Affairs.

EC–6997. A communication from the Attorney, Office of the General Counsel, Bureau of Consumer Financial Protection, transmitting, pursuant to law, the report of a rule entitled ''Confidential Treatment of Privileged Information'' ((RIN3170–AA20) (Docket No. CFPB–2012–0010)) received in the Office of the President of the Senate on July 25, 2012; to the Committee on Banking, Housing, and Urban Affairs.

EC–6998. A communication from the Chief Counsel, Federal Emergency Management Agency, Department of Homeland Security, transmitting, pursuant to law, the report of a rule entitled ''Suspension of Community Eligibility'' ((44 CFR Part 64) (Docket No. FEMA–2012–0003)) received in the Office of the President of the Senate on July 25, 2012; to the Committee on Banking, Housing, and Urban Affairs.

EC–6999. A communication from the Comptroller of the Currency, transmitting, pursuant to law, a report relative to Section 322(k) of the Dodd-Frank Wall Street Reform and Consumer Protection Act; to the Committee on Banking, Housing, and Urban Affairs.

EC–7000. A communication from the Secretary of the Treasury, transmitting, pursuant to law, a report relative to the Financial Stability Oversight Council's study of the feasibility, benefits, costs, and structure of a contingent capital requirement for nonbank financial companies; to the Committee on Banking, Housing, and Urban Affairs.

EC–7001. A communication from the Secretary of the Treasury, transmitting, pursuant to law, the Financial Stability Oversight Council's annual report to Congress on the activities of the Council; to the Committee on Banking, Housing, and Urban Affairs.

EC–7002. A communication from the Senior Vice President and Chief Financial Officer, Federal Home Loan Bank of New York, transmitting, pursuant to law, the Bank's 2011 Management Report; to the Committee on Banking, Housing, and Urban Affairs.

EC–7003. A communication from the Principal Deputy Under Secretary of Defense (Personnel and Readiness), transmitting the report of an officer authorized to wear the insignia of the grade of brigadier general in accordance with title 10, United States Code, section 777; to the Committee on Armed Services.

EXECUTIVE REPORTS OF COMMITTEE

The following executive reports of nominations were submitted:

By Mr. KERRY for the Committee on Foreign Relations.

*Gene Allan Cretz, of New York, a Career Member of the Senior Foreign Service, Class of Minister-Counselor, to be Ambassador Extraordinary and Plenipotentiary of the United States of America to the Republic of Ghana.

Nominee: Gene Allan Cretz.

Post: Ambassador to Ghana.

(The following is a list of all members of my immediate family and their spouses. I have asked each of these persons to inform me of the pertinent contributions made by them. To the best of my knowledge, the information contained in this report is complete and accurate.)

Contributions, amount, date, and donee:

1. Self: None. 0
2. Spouse: None. 0
3. Children and Spouses: None. 0
4. Parents: None. 0
5. Grandparents: None. 0
6. Brothers and Spouses: None. 0
7. Sisters and Spouses: None. 0

---

*Deborah Ruth Malac, of Virginia, a Career Member of the Senior Foreign Service, Class of Counselor, to be Ambassador Extraordinary and Plenipotentiary of the United States of America to the Republic of Liberia.

Nominee: Deborah Ruth Malac.

Post: Liberia.

(The following is a list of all members of my immediate family and their spouses. I have asked each of these persons to inform me of the pertinent contributions made by them. To the best of my knowledge, the information contained in this report is complete and accurate.)

Contributions, amount, date, and donee:

1. Self: $150.00, 06/20/2008, Friends of Mark Warner.

2. Spouse: $35.00, 02/18/2009, Democratic National Committee; $35.00, 03/19/2009, Democratic National Committee.

3. Children and Spouses: Nicholas Stefan Olson: $107.07, 11/03/2008, Obama Victory Fund; $30,00, 11/05/2008, Obama Victory Fund. Gregory Michael Olson: None. Katharine Elaine Olson: None.

4. Parents: Barry Forrest Malac and Marian Bartak Malac: $25.00, 01/10/2008, Georgia Republican Party; $20.00, 01/22/2008, Union County (GA) Republican Women; $15.00, 06/07/2008, Republican National Committee; $10.00, 08/14/2008, RNC Victory 2008; $20.00, 1/17/2008, Republican National Committee; $20.00, 01/23/2009, Union County (GA) Republican Women; $10.00, 07/15/2009, Georgia Republican Party; $10.00, 09/28/2009, Republican National Committee; $15.00, 10/21/2009, Republican National Committee; $20.00, 01/23/2010, Union County (GA) Republican Women; $20.00, 04/17/2010, Republican National Committee; $10.00, 09/10/2010, Republican National Committee; $15.00, 10/06/2010, National Republican Congressional Committee; $15.00, 10/30/2010, National Republican Committee; $15.00, 04/04/2011, National Republican Congressional Committee; $25.00, 06/21/2011, Union County (GA) Republican Women; $15.00, 11/02/2011, National Republican Congressional Committee.

5. Grandparents: Rev. Joseph Paul Bartak—deceased; Minnie Polk Bartak—deceased; Rev. Gustav Malac—deceased; Antonie Malac—deceased.

6. Brothers and Spouses: Roy David Malac and Carolyn Malac: None; Timothy Alan Malac and Theresa Malac: None.

7. Sisters and Spouses: None.

---

*Thomas Hart Armbruster, of New York, a Career Member of the Senior Foreign Service, Class of Counselor, to be Ambassador Extraordinary and Plenipotentiary of the United States of America to the Republic of the Marshall Islands.

Nominee: Thomas Hart Armbruster.

Post: Chief of Mission Marshall Islands.

(The following is a list of all members of my immediate family and their spouses. I have asked each of these persons to inform me of the pertinent contributions made by them. To the best of my knowledge, the information contained in this report is complete and accurate.)

Contributions, amount, date, and donee:

1. Self: None.

2. Spouse: None.

3. Children and Spouses; Son: Bryan Christopher Armbruster: None. Daughter: Kalia Chandler Armbruster: $20, 2010, Obama for America.

4. Parents: Father: Robert John Armbruster: None. Mother: Nancy Elizabeth Armbruster: $20, 2010, Obama for America.

5. Grandparents: None.

6. Brothers and Spouses: Brother: Christopher Ian Armbruster: $40, 2010, Obama for America. Spouse: Carol Benson: None.

7. Sisters and Spouses: None.

---

*David Bruce Wharton, of Virginia, a Career Member of the Senior Foreign Service, Class of Minister-Counselor, to be Ambassador Extraordinary and Plenipotentiary of the United States of America to the Republic of Zimbabwe.

NOMINEE: David Bruce Wharton.

POST: Zimbabwe.

(The following is a list of all members of my immediate family and their spouses. I have asked each of these persons to inform me of the pertinent contributions made by them. To the best of my knowledge, the information contained in this report is complete and accurate.)

Contributions, amount, date, and donee:

1. Self: $25, 5/25/08, ''Obama for America''; $50, 7/4/08, ''Obama for America''; $50, 10/15/08, ''Obama for America''; $25, 6/30/11, ''Obama for America''; $25, 9/14/11, ''Obama for America''; $50, 12/20/11, ''Gerry Connolly for Congress.''

2. Spouse: $25, 6/25/08, ''Obama for America''; $25, 10/15/08, ''Obama for America''; $25, 2/14/12, ''Obama for America''; $25, 05/08/12, ''Gerry Connolly for Congress.''

3. Children and Spouses: None.

4. Parents: CM Wharton, Approx $200 06/08 to 04/12, ''Obama for America.''

5. Grandparents: None.

6. Brothers and Spouses: None.

7. Sisters and Spouses: None.

---

*Greta Christine Holtz, of Maryland, a Career Member of the Senior Foreign Service, Class of Minister-Counselor, to be Ambassador Extraordinary and Plenipotentiary of the United States of America to the Sultanate of Oman.

Nominee: Greta C. Holtz.

Post: Oman.

(The following is a list of all members of my immediate family and their spouses. I have asked each of these persons to inform me of the pertinent contributions made by them. To the best of my knowledge, the information contained in this report is complete and accurate.)

Contributions, amount, date, and donee:

1. Self: None.

2. Spouse: Francisco Cosio-Marron. None.

3. Children and Spouses: Victoria Cosio-Marron: None; Alexandra Cosio-Marron: None; Anthony Cosio-Marron: None.

4. Parents: Frederick C. Holtz, Jr.: None; Clarice C. Holtz: None.

5. Grandparents: Carlos W. Campbell: None; Alice M. Campbell: None; Frederick C. Holtz: None; Margaret N. Holtz: None.

6. Brothers and Spouses: Frederick C. Holtz: None; Denise Holtz: None.

7. Sisters and Spouses: Carla E. Holtz: None.

---

*Alexander Mark Laskaris, of Maryland, a Career Member of the Senior Foreign Service, Class of Counselor, to be Ambassador Extraordinary and Plenipotentiary of the United States of America to the Republic of Guinea.

Nominee: Alexander M. Laskaris.

Post: Republic of Guinea.

(The following is a list of all members of my immediate family and their spouses. I have asked each of these persons to inform me of the pertinent contributions made by them. To the best of my knowledge, the information contained in this report is complete and accurate.)

Contributions, amount, date, and donee:

1. Self: None.

2. Spouse: N/A.

3. Children and Spouses: N/A.

4. Parents: Gus C.A. Laskaris—deceased, None; Evelyn Laskaris: None.

5. Grandparents: Anthony & Katherine Xanthopoulos—deceased, None; Arisitidis & Eleni Laskaris, deceased; None.

6. Brothers and Spouses: Anthony Laskaris: $50, 2008, Democratic National Cmte; $50, 2009, Democratic National Cmte; $50, 2010, Democratic National Cmte; $50, 2011, Democratic National Cmte; $50, 2012, Democratic National Cmte.

Gus A. Laskaris: None.

7. Sisters and Spouses: Maria Laskaris: $100, 2008, Hillary Clinton for President.

---

*Marcie B. Ries, of the District of Columbia, a Career Member of the Senior Foreign Service, Class of Career-Minister, to be Ambassador Extraordinary and Plenipotentiary of the United States of America to the Republic of Bulgaria.

Nominee: Marcie B. Ries.

Post: Ambassador to the Republic of Bulgaria.

Nominated: May 24, 2012.

(The following is a list of all members of my immediate family and their spouses. I have asked each of these persons to inform me of the pertinent contributions made by them. To the best of my knowledge, the information contained in this report is complete and accurate.)

Contributions, amount, date, and donee:

1. Self: None.

2. Spouse: $250, 6/1/2011, Elizabeth Esty.

3. Children and Spouses: Alexander, none; Meredith, none.

4. Parents: Mona Berman: $75, 2008, Dem Natl Comm; $50, 2009, DNC; $75, 2010, DNC; $50, 2010, Emily's List.

5. Grandparents: Deceased.

6. Brothers and Spouses: None.

7. Sisters and Spouses: Laura Jane Berman, none.

---

*John M. Koenig, of Washington, a Career Member of the Senior Foreign Service, Class of Minister-Counselor, to be Ambassador Extraordinary and Plenipotentiary of the United States of America to the Republic of Cyprus.

Nominee: John M. Koenig.

Post: Ambassador to the Republic of Cyprus.

Nominated: June 6, 2012.

(The following is a list of all members of my immediate family and their spouses. I nave asked each of these persons to inform me of the pertinent contributions made by them. To the best of my knowledge, the information contained in this report is complete and accurate.)

Contributions, amount, date, and donee:

1. Self: $250,00, 10-05-2008, Obama for America.

2. Spouse: Natalie, none.

3. Children and Spouses: Theodore—single, none; Alexander—single, none.

4. Parents: Theodore Koenig, Janet Koenig—deceased, none.

5. Grandparents: Gerald Crowe—deceased, none; Bernice Crowe—deceased, none; John F. Koenig—deceased, none; Martha Koenig—deceased, none.

6. Brothers and Spouses: N/A.

7. Sisters and Spouses: Kathryn Emrick: $100.00, 09-19-2008, Obama for America; $50.00, 11-01-2008, Obama for America; Max Emrick: $50.00, 10-30-2011, Maria Cantwell; Lisa Koenig, none; Matthew Baker, none.

---

*Michael David Kirby, of Virginia, a Career Member of the Senior Foreign Service, Class of Minister-Counselor, to be Ambassador Extraordinary and Plenipotentiary of the United States of America to the Republic of Serbia.

Nominee: Michael D. Kirby.

Post: Ambassador to the Republic of Serbia.

Nominated: June 14, 2012.

(The following is a list of all members of my immediate family and their spouses. I have asked each of these persons to inform me of the pertinent contributions made by them. To the best of my knowledge, the information contained in this report is complete and accurate.)

Contributions, amount, date, and donee:

1. Self: $40, 2010, Congressman Gerry Connelly.

2. Spouse: Sara Powelson Kirby, none.

3. Children and Spouses: Katherine Van Nest Kirby—daughter, none; Enrique Plaza Garcia—her husband, none; Elizabeth Marie Kirby—daughter, none.

4. Parents: Dolores Marie Kirby: $50, 2007, 2008, & 2009, DNC; $200, 2008, Obama for America; Richard Norman Kirby—deceased.

5. Grandparents: Charles and Marie Senkfor—both deceased; James P. and Marie Kirby—both deceased.

6. Brothers and Spouses: Charles J. Kirby: $100, 2008, MoveOn.org; $100, 2008, Obama for America; Christie Kramer (his spouse), none; Richard A. Kirby and his spouse Beth-ann Roth, none.

7. Sisters and Spouses: Lynn Marie Kirby and her spouse Stephen Rogers, none.

Mr. KERRY. Mr. President, for the Committee on Foreign Relations I report favorably the following nomination lists which were printed in the RECORDS on the dates indicated, and ask unanimous consent, to save the expense of reprinting on the Executive Calendar that these nominations lie at the Secretary's desk for the information of Senators.

The PRESIDING OFFICER. Without objection, it is so ordered.

Foreign Service nominations beginning with Narendran Chanmugam and ending with Jana S. Wooden, which nominations were received by the Senate and appeared in the Congressional Record on June 7, 2012.

Foreign Service nominations beginning with Thomas J. Brennan and ending with Thomas Pepe, which nominations were received by the Senate and appeared in the Congressional Record on June 20, 2012.

*Nomination was reported with recommendation that it be confirmed subject to the nominee's commitment to respond to requests to appear and testify before any duly constituted committee of the Senate.

(Nominations without an asterisk were reported with the recommendation that they be confirmed.)

INTRODUCTION OF BILLS AND JOINT RESOLUTIONS

The following bills and joint resolutions were introduced, read the first and second times by unanimous consent, and referred as indicated:

By Mr. BROWN of Ohio:

S. 3444. A bill to require that textile and apparel articles acquired for use by executive agencies be manufactured from articles, materials, or supplies entirely grown, produced, or manufactured in the United States; to the Committee on Homeland Security and Governmental Affairs.

By Mr. HOEVEN (for himself, Mr. MCCONNELL, Ms. MURKOWSKI, Mr. BARRASSO, Mr. CORNYN, Mr. VITTER, Mr. THUNE, Mr. BLUNT, Mr. WICKER, Mrs. HUTCHISON, Mr. BURR, Mr. HELLER, Mr. RISCH, Mr. COATS, Mr. PORTMAN, Mr. KYL, Mr. SESSIONS, Mr. SHELBY, Mr. INHOFE, Mr. COCHRAN, Mr. MCCAIN, Mr. ISAKSON, Mr. CRAPO, Mr. ENZI, Mr. ROBERTS, Mr. BOOZMAN,

Mr. COBURN, Mr. JOHNSON of Wisconsin, Mr. CHAMBLISS, Mr. JOHANNS, and Mr. LUGAR):

S. 3445. A bill to approve the Keystone XL Pipeline, to provide for the development of a plan to increase oil and gas exploration, development, and production under oil and gas leases of Federal land, and for other purposes; to the Committee on Energy and Natural Resources.

By Mr. CORNYN:

S. 3446. A bill to amend the Endangered Species Act of 1973 to halt the premature proposed listing of 4 central Texas salamander species resulting from a settlement agreement, and to take into account extensive ongoing State and local conservation efforts; to the Committee on Environment and Public Works.

By Mr. FRANKEN (for himself and Ms. KLOBUCHAR):

S. 3447. A bill to amend the Employee Retirement Income Security Act of 1974 to permit access to certain disability benefits without penalty; to the Committee on Health, Education, Labor, and Pensions.

By Mrs. HAGAN (for herself and Mr. BURR):

S. 3448. A bill to direct the Secretary of the Interior to enter into an agreement to provide for management of the free-roaming wild horses in and around the Currituck National Wildlife Refuge; to the Committee on Environment and Public Works.

By Ms. STABENOW (for herself and Mr. GRAHAM):

S. 3449. A bill to prohibit purchases by the Federal Government of Chinese goods and services until the People's Republic of China becomes a party to the Agreement on Government Procurement, and for other purposes; to the Committee on Homeland Security and Governmental Affairs.

By Mr. COATS (for himself, Mr. BARRASSO, Mr. ENZI, Mr. INHOFE, Mr. HOEVEN, Mr. LEE, Mr. COCHRAN, Mr. COBURN, Mr. RISCH, Mr. CRAPO, Mr. PAUL, Mr. MCCONNELL, Mr. HATCH, Mr. SESSIONS, Mr. WICKER, Mr. BOOZMAN, Mr. MCCAIN, Mr. BURR, Mr. ISAKSON, and Mr. CHAMBLISS):

S. 3450. A bill to limit the authority of the Secretary of the Interior to issue regulations before December 31, 2013, under the Surface Mining Control and Reclamation Act of 1977; to the Committee on Energy and Natural Resources.

By Mr. BEGICH:

S. 3451. A bill to exempt certain air taxi services from taxes on transportation by air; to the Committee on Finance.

By Mr. DURBIN (for himself, Mrs. BOXER, Mr. MERKLEY, and Mr. WHITEHOUSE):

S. 3452. A bill to amend the Truth in Lending Act to establish a national usury rate for consumer credit transactions; to the Committee on Banking, Housing, and Urban Affairs.

By Mr. HARKIN (for himself, Ms. MIKULSKI, Mrs. MURRAY, Mr. SANDERS, Mr. MERKLEY, Mr. FRANKEN, Mr. BLUMENTHAL, Mr. LEAHY, Mr. AKAKA, Mrs. BOXER, Mr. WYDEN, Mr. DURBIN, Mr. SCHUMER, Mr. LAUTENBERG, Mr. BROWN of Ohio, and Mrs. GILLIBRAND):

S. 3453. A bill to provide for an increase in the Federal minimum wage; to the Committee on Health, Education, Labor, and Pensions.

SUBMISSION OF CONCURRENT AND SENATE RESOLUTIONS

The following concurrent resolutions and Senate resolutions were read, and referred (or acted upon), as indicated:

By Mr. KERRY (for himself, Mr. CHAMBLISS, Mr. INOUYE, Mr. WYDEN, Mr. AKAKA, and Mr. CARDIN):

S. Res. 529. A resolution recognizing that the occurrence of prostate cancer in African-American men has reached epidemic proportions and urging Federal agencies to address that health crisis by supporting education, awareness outreach, and research specifically focused on how prostate cancer affects African-American men; considered and agreed to.

By Mrs. MURRAY (for herself, Mr. HARKIN, Mr. JOHNSON of Wisconsin, Mr. KOHL, Mr. BLUMENTHAL, Mr. PRYOR, and Ms. CANTWELL):

S. Res. 530. A resolution designating the month of August 2012 as ''National Registered Apprenticeship Month''; considered and agreed to.

By Ms. KLOBUCHAR (for herself, Mr. HATCH, Mr. BENNET, Mr. ISAKSON, Mr. DURBIN, and Mr. MERKLEY):

S. Res. 531. A resolution commemorating the success of Team USA in the past 25 Olympic Games and supporting Team USA in the 2012 Olympic and Paralympic Games; considered and agreed to.

By Mr. NELSON of Florida (for himself, Mr. RUBIO, Mr. DURBIN, Mr. LEAHY, Ms. CANTWELL, Mr. LAUTENBERG, Mr. SESSIONS, Mr. ENZI, Mr. CARDIN, Ms. MIKULSKI, Ms. LANDRIEU, and Mr. KOHL):

S. Res. 532. A resolution expressing support for the XIX International AIDS Conference and the sense of the Senate that continued commitment by the United States to HIV/AIDS research, prevention, and treatment programs is crucial to protecting global health; considered and agreed to.

ADDITIONAL COSPONSORS

S. 195

At the request of Mr. ROCKEFELLER, the name of the Senator from Rhode Island (Mr. REED) was added as a cosponsor of S. 195, a bill to reinstate Federal matching of State spending of child support incentive payments.

S. 1173

At the request of Mr. WYDEN, the name of the Senator from Washington (Ms. CANTWELL) was added as a cosponsor of S. 1173, a bill to amend title XVIII of the Social Security Act to modernize payments for ambulatory surgical centers under the Medicare program.

S. 1299

At the request of Mr. MORAN, the name of the Senator from South Dakota (Mr. JOHNSON) was added as a cosponsor of S. 1299, a bill to require the Secretary of the Treasury to mint coins in commemoration of the centennial of the establishment of Lions Clubs International.

S. 1454

At the request of Mr. DURBIN, the name of the Senator from Connecticut (Mr. LIEBERMAN) was added as a cosponsor of S. 1454, a bill to amend title XVIII of the Social Security Act to provide for extended months of Medicare coverage of immunosuppressive drugs for kidney transplant patients and other renal dialysis provisions.

S. 1935

At the request of Mrs. HAGAN, the names of the Senator from Wisconsin (Mr. KOHL), the Senator from Colorado (Mr. BENNET), the Senator from Washington (Mrs. MURRAY), the Senator from Pennsylvania (Mr. CASEY), the Senator from Connecticut (Mr. LIEBERMAN) and the Senator from Nevada (Mr. HELLER) were added as cosponsors of S. 1935, a bill to require the Secretary of the Treasury to mint coins in recognition and celebration of the 75th anniversary of the establishment of the March of Dimes Foundation.

S. 1990

At the request of Mr. LIEBERMAN, the name of the Senator from Pennsylvania (Mr. CASEY) was added as a cosponsor of S. 1990, a bill to require the Transportation Security Administration to comply with the Uniformed Services Employment and Reemployment Rights Act.

S. 2055

At the request of Mr. SHELBY, the names of the Senator from Georgia (Mr. CHAMBLISS) and the Senator from Georgia (Mr. ISAKSON) were added as cosponsors of S. 2055, a bill to amend the Federal Deposit Insurance Act with respect to the protection of certain information.

S. 2078

At the request of Mr. MENENDEZ, the name of the Senator from Florida (Mr. RUBIO) was added as a cosponsor of S. 2078, a bill to enable Federal and State chartered banks and thrifts to meet the credit needs of the Nation's home builders, and to provide liquidity and ensure stable credit for meeting the Nation's need for new homes.

S. 2094

At the request of Mr. BROWN of Ohio, the name of the Senator from Michigan (Mr. LEVIN) was added as a cosponsor of S. 2094, a bill to amend the Federal Water Pollution Control Act to update a program to provide assistance for the planning, design, and construction of treatment works to intercept, transport, control, or treat municipal combined sewer overflows and sanitary sewer overflows, and to require the Administrator of the Environmental Protection Agency to update certain guidance used to develop and determine the financial capability of communities to implement clean water infrastructure programs.

S. 2268

At the request of Mrs. GILLIBRAND, the name of the Senator from New York (Mr. SCHUMER) was added as a cosponsor of S. 2268, a bill to ensure that all items offered for sale in any gift shop of the National Park Service or of the National Archives and Records Administration are produced in the United States, and for other purposes.

S. 2472

At the request of Mr. CASEY, the name of the Senator from Missouri (Mr. BLUNT) was added as a cosponsor of S. 2472, a bill to provide for the issuance and sale of a semipostal by the United States Postal Service for research and demonstration projects relating to autism spectrum disorders.

S. 3204

At the request of Mr. JOHANNS, the names of the Senator from Alabama (Mr. SHELBY) and the Senator from New Hampshire (Ms. AYOTTE) were added as cosponsors of S. 3204, a bill to address fee disclosure requirements under the Electronic Fund Transfer Act, and for other purposes.

S. 3239

At the request of Mrs. FEINSTEIN, the name of the Senator from California (Mrs. BOXER) was added as a cosponsor of S. 3239, a bill to provide for a uniform national standard for the housing and treatment of egg—laying hens, and for other purposes.

S. 3326

At the request of Mr. JOHANNS, his name was added as a cosponsor of S. 3326, a bill to amend the African Growth and Opportunity Act to extend the third—country fabric program and to add South Sudan to the list of countries eligible for designation under that Act, to make technical corrections to the Harmonized Tariff Schedule of the United States relating to the textile and apparel rules of origin for the Dominican Republic—Central America—United States Free Trade Agreement, to approve the renewal of import restrictions contained in the Burmese Freedom and Democracy Act of 2003, and for other purposes.

S. 3428

At the request of Mr. CARDIN, the name of the Senator from Arkansas (Mr. BOOZMAN) was added as a cosponsor of S. 3428, a bill to amend the Clean Air Act to partially waive the renewable fuel standard when corn inventories are low.

S. 3436

At the request of Mr. FRANKEN, the name of the Senator from Alaska (Mr. BEGICH) was added as a cosponsor of S. 3436, a bill to amend the Child Care and Development Block Grant Act of 1990 to improve the quality of infant and toddler care.

S. 3442

At the request of Ms. LANDRIEU, the names of the Senator from Oregon (Mr. MERKLEY), the Senator from Connecticut (Mr. BLUMENTHAL), the Senator from New York (Mrs. GILLIBRAND), the Senator from Rhode Island (Mr. WHITEHOUSE), the Senator from California (Mrs. BOXER), the Senator from New Hampshire (Mrs. SHAHEEN) and the Senator from Maryland (Mr. CARDIN) were added as cosponsors of S. 3442, a bill to provide tax incentives for small businesses, improve programs of the Small Business Administration, and for other purposes.

S.J. RES. 39

At the request of Mr. CARDIN, the name of the Senator from Hawaii (Mr. AKAKA) was added as a cosponsor of S.J. Res. 39, a joint resolution removing the deadline for the ratification of the equal rights amendment.

S. CON. RES. 48

At the request of Mr. LEAHY, the name of the Senator from Vermont (Mr. SANDERS) was added as a cosponsor of S. Con. Res. 48, a concurrent resolution recognizing 375 years of service of the National Guard and affirming congressional support for a permanent Operational Reserve as a component of the Armed Forces.

S. RES. 176

At the request of Ms. MIKULSKI, the name of the Senator from Montana (Mr. TESTER) was added as a cosponsor of S. Res. 176, a resolution expressing the sense of the Senate that the United States Postal Service should issue a semipostal stamp to support medical research relating to Alzheimer's disease.

STATEMENTS ON INTRODUCED BUS AND JOINT RESOLUTIONS

By Mr. HOEVEN (for himself, Mr. MCCONNELL, Ms. MURKOWSKI, Mr. BARRASSO, Mr. CORNYN, Mr. VITTER, Mr. THUNE, Mr. BLUNT, Mr. WICKER, Mrs. HUTCHISON, Mr. BURR, Mr. HELLER, Mr. RISCH, Mr. COATS, Mr. PORTMAN, Mr. KYL, Mr. SESSIONS, Mr. SHELBY, Mr. INHOFE, Mr. COCHRAN, Mr. MCCAIN, Mr. ISAKSON, Mr. CRAPO, Mr. ENZI, Mr. ROBERTS, Mr. BOOZMAN, Mr. COBURN, Mr. JOHNSON, of Wisconsin, Mr. CHAMBLISS, Mr. JOHANNS, and Mr. LUGAR):

S. 3445. A bill to approve the Keystone XL Pipeline, to provide for the development of a plan to increase oil and gas exploration, development, and production under oil and gas leases of Federal land, and for other purposes; to the Committee on Energy and Natural Resources.

Mr. HOEVEN. Mr. President, I rise to discuss this comprehensive plan for energy security for our Nation.

When I say ''energy security,'' I mean producing more energy than we consume. I believe, with this approach, within 5 to 7 years we can truly be a nation that is energy secure. Again, I mean producing more energy than we consume. This comprehensive plan for energy security is about truly producing all our energy resources in this country.

Many of these bills in this package of Energy bills have already been passed by the House that we are introducing now in the Senate, as well as additional legislation—ideas that Senators have put forward that were adding to it as well.

The approach is similar to the approach we have taken in North Dakota over the last decade. My home State of North Dakota has developed all its energy resources—both traditional and renewable—in a vigorous way over the last decade, and we are now an energy powerhouse for the Nation. We can see what we are doing in oil and gas, but we are doing a tremendous amount in all other forms of energy as well—both traditional and renewable. It is because we worked in a very inclusive way to include everybody's ideas in building a comprehensive energy plan that we call Empower ND—Empower North Dakota.

There was no one person who came up this whole comprehensive plan or with all the ideas, but we reached out to everyone—all the different energy sectors—and said: Let's collaborate, let's work together, let's pass a comprehensive energy plan, and then let's keep improving it. Let's make it a process rather than a one-time product and keep adding ideas and bringing forth items that will help us spur and drive our energy development in the State, ideas that will create the kind of business climate that will truly empower private investment—private investment that will deploy the new technologies that not only produce more energy but do it with sound environmental stewardship. That is exactly what is happening in North Dakota, and that is exactly what need to do at the national level.

This Domestic Energy and Jobs Act clearly demonstrates that we have an energy plan and that we are ready to go and that we are coordinating with our colleagues in the House as well. Right now there are 30 sponsors for this legislation, including the Republican leadership, as well as the energy leaders.

It also is a plan which has reached out to what the House calls their HEAT team—which stands for House Energy Action Team. Representative MCCARTHY and others, certainly FRED UPTON, who is head of their Energy and Commerce Committee, Representative HASTINGS, and others who are truly energy leaders in the House—people whom I have worked with on things such as the Keystone Pipeline, Representative TERRY and Representative CONNIE MACK and others.

This is about getting people involved in an inclusive way and putting in place an energy policy that truly serves this Nation and empowers private investment. We see how important that is now.

We have hundreds of billions of investment dollars waiting to be invested in producing more energy, more jobs, and more security for our country. This approach will empower private investment to develop all our energy resources. It does things such as reduce the regulatory burden, streamlines permitting—both onshore and offshore—and helps us develop vital infrastructure such as the Keystone Pipeline. It develops our resources on public lands, including our renewables, and setting realistic goals with a market-based approach, not picking winners or losers, and preserving multiple use on our public lands throughout this country. It would put in a freeze and require a study of rules that are driving up our gasoline prices.

It also includes a bill from Senator MURKOWSKI. It directs the U.S. Geological Survey to establish an inventory of critical minerals in the United States and to set policies to help us develop those minerals.

What is the impact? The U.S. Chamber of Commerce, in March of 2011, undertook a study. In that study, they looked and determined there are more

than 350 energy projects that are being held up because of an inability to get permitted or a regulatory burden or other hurdles and roadblocks. In that study, they determined that if these energy projects—again, more than 350 energy projects—could be green-lighted, it would $1.1 trillion in additional gross domestic product and 1.9 million jobs a year—1.9 million jobs a year just in the construction phase for those energy projects.

So this legislation isn't just about energy for our country. It is about energy. It is about a comprehensive approach—more than 13 different pieces of legislation, many of which have already passed the House. It is about a comprehensive approach to get development of our energy resources underway in a big way. But it is about job creation. It is about economic growth. It is about economic growth that will help us get the 13 million-plus people who are currently unemployed back to work. It is about economic growth that will help us generate revenue to reduce our deficit and our debt, and it truly is about national security.

Look what is going on right now in the Middle East. Look what is going on in Syria, in Iran, in Egypt with the rise of the Muslim Brotherhood. Look at the instability. Yet we still depend on oil from the Middle East and places such as Venezuela. There is no need for that. We can produce our own energy and more. It is an interconnected world. We all know that.

So when I talk about energy security, I mean producing more energy than we consume. That is what I mean by energy security. Of course, when there is an increased supply, what happens? It helps bring prices down. Think of the impact that has for families and for our economy.

Just recently, in the last few days, a company called CNOOC out of China—which is essentially a Chinese Government-owned company—offered $15 billion to buy Nexen, a major Canadian oil company—$15 billion. Why did they do that? To buy energy resources in Canada, so China would own energy resources in Canada.

As you know, I have been down on the floor many times, and I have worked very hard to get the Keystone Pipeline approved because if we don't produce and get that oil from Canada, somebody else will, and China is working to do just that.

So after the administration held up the Keystone XL Pipeline, what happened? Canadian Prime Minister Harper went to China. There, he met with Chairman Wu and the other energy leaders in China and they signed an MOU or MOA, a memorandum of understanding/memorandum of agreement.

In it, what did they say? They said China and Canada are going to cooperate on developing resources, energy resources in Canada. Of course, that energy then goes to China.

The question we have to ask is are we going to work with our closest friend and ally, Canada, to develop things such as the Keystone XL Pipeline so oil will come from Canada to the United States rather than going to China.

Or are we in this country going to be in a position where we have to buy our oil back from the Chinese? I know how the Americans want that question answered. That is what I am talking about. We need to be developing these energy resources in this country, and together with our closest friend and ally, Canada, we can do it.

There is another important point to be made here. I know there are some opponents of developing the Canadian oil sands concerned about CO_2 emissions. But here are some things they have to think about. Already you can see China coming in, working with Canada to develop those resources. So those resources are going to be developed. The question is, is that oil going to China or is it going to come to the United States?

The point is this: By building pipelines, we not only bring it to the United States but we empower investment in the Canadian oil sands that will help us produce more energy but do it with better environmental stewardship. Eighty percent of the new development in the Canadian oil sands is what is called ''in situ,'' which means drilling instead of the excavation. That means lower CO_2 emissions, that means emissions very much in line with what we produce now in the United States with our conventional drilling.

We have an opportunity, an incredible opportunity. We need to seize it with both hands. As I say, we can be energy secure in this country within 5 years. I think when people look at what is going on in the Middle East, when they see our soldiers over there, when they see the instability that is being created by regimes like Syria or Iran, when they see what is going on in countries like Egypt and they understand there could be an event that closes the Strait of Hormuz, they understand what that would mean for oil prices and energy prices in this country.

We do not want to be dependent on that situation, which means it is time to act. This is not about spending money; this is about generating jobs and generating revenue that will help us reduce our deficit, that will put our people to work, that will unleash the private investment, the entrepreneurship, the ingenuity of the American people to truly propel our Nation forward, to propel our economy forward, and to make us safer and more secure. The time has come to act. The House passed much of this plan with bipartisan support. We need to do the same in the Senate.

This is not the end of the story. This is an important part, the foundation, if you will, of building the right energy story for our country. We can do it and I urge my colleagues to join me in this effort.

By Mr. DURBIN (for himself, Mrs. BOXER, Mr. MERKLEY, and Mr. WHITEHOUSE):

S. 3452. A bill to amend the Truth in Lending Act to establish a national usury rate for consumer credit transactions; to the Committee on Banking, Housing, and Urban Affairs.

Mr. DURBIN. Mr. President, as our economy continues to recover, families across America are still facing financial hardships. Our priority to help working families must persevere, and we must protect them from future financial harm.

Some have compared today's predatory lending practices to the subprime lending that caused the financial crisis in 2008. We need to free our financial system from these abuses and prevent consumers from never-ending debt traps.

Today I am introducing the Protecting Consumers from Unreasonable Credit Rates Act to protect consumers from aggressive predatory lending practices. The bill caps annualized interest rates on consumer credit at 36 percent.

Consumers spend over $30 billion every year on predatory payday loans, high-cost overdraft loans, and other forms of credit. Imagine if a portion of that $300 billion ten-year cost of credit could be redirected towards buying American goods and services.

In an era that has called for trillions of taxpayer dollars to bail out banks and jumpstart economic demand, this proposal costs the taxpayers nothing. In fact, in the case of payday lending, it could potentially save billions of dollars in fees and interest paid by the 12 million American taxpayers who use these products annually.

The Protecting Consumers from Unreasonable Credit Rates Act would establish a new federal annualized Fee and Interest Rate calculation—the FAIR—and institute a 36 percent cap for all types of consumer credit.

In 2006, Congress enacted a Federal 36 percent annualized usury cap for certain credit products marketed to military servicemembers and their families, which curbed payday, car title, and other forms of credit around military bases. My bill would provide the same protections for all Americans.

Although I hope to gain widespread support for this bill from responsible lenders, I understand that some of the financial service firms in this country will be uneasy with a broad bill establishing a high interest rate cap.

There are those that will claim it is not possible to create a profitable, small-dollar, short-term loan with APR capped at 36 percent and consumer protections. However, there are financial institutions that currently offer access to quick credit through products with consumer protections and interest less than 36 percent. I hope with the introduction of this bill we can open an honest conversation about consumer credit rates and how it impacts American families.

I would first start by asking what services these firms provide that can justify charging customers over 36 percent in annual interest. How do lenders in my home state of Illinois justify charging annual rates over 400 percent? In my opinion, there is no justification.

Consider 66 year-old Rosa Mobley, who lives on Social Security and a small pension.

The Chicago Tribune reports that Ms. Mobley took out a car title loan—a type of payday loan in which the borrowers put up their cars as collateral—for $1,000. Ms. Mobley was charged 300 percent interest.

She wound up paying more than $4,000 over 28 months and at the time of the report was struggling just to get by.

This bill would require that all fees and finance changes be included in the new usury rate calculation and would require all lending to conform to the limit, thereby eliminating the many loopholes that have allowed these predatory practices to flourish.

It would not preempt stronger state laws, it would allow states' attorneys general to help enforce this new rate cap, and it would provide for strong civil penalties to deter lender violations.

The Protecting Consumers from Unreasonable Credit Rates Act would eliminate predatory lenders, as well as would help borrowers make smarter choices.

The Truth in Lending Act was enacted over 40 years ago to help consumers compare the costs of borrowing when buying a home, a car, or other items by establishing a standard Annual Percentage Rate that all lenders should advertise.

My first mentor in politics, the late Senator Paul Douglas from my home state of Illinois, said all the way back in 1963 that too often lenders:

compound the camouflaging of credit by loading on all sorts of extraneous fees, such as exorbitant fees for credit life insurance, excessive fees for credit investigation, and all sorts of loan processing fees which rightfully should be included in the percentage rate statement so that any percentage rate quoted is meaningless and deceptive.

That was before anyone had ever heard of ''subprime lending.''

Unfortunately, as the use of credit has exploded and as the complexity of the credit products offered by lenders has become mind-boggling, Congress and the Federal Reserve have taken several actions since the passage of Truth in Lending to weaken the APR as a tool for comparison shopping. Today, many fees can be excluded from the rate that is given to borrowers. The APR no longer gives consumers the convenient and accurate information it once did.

This bill would give consumers a way to accurately compare credit options, by requiring that the new FAIR calculation be disclosed both for open-end credit plans such as credit cards and for closed-end credit such as mortgages and payday loans.

On a related note, I commend my colleague, Senator JEFF MERKLEY of Oregon, who introduced the SAFE Lending Act of 2012 earlier this week. I am proud to be an original cosponsor of the bill. The bill would require better compliance among lenders within existing laws and provide new enforcement measures for offshore lenders or those who claim the right to tribal sovereign immunity. These provisions, along with further consumer protections offered within his bill, offer much-needed lending reforms.

Various Federal and State loopholes allow unscrupulous lenders to charge struggling consumers 400 percent annual interest for payday loans on average, 300 percent annual interest for car title loans, up to 3500 percent annual interest for bank overdraft loans, and triple-digit rates for online installment loans.

As Congress continues to address economic challenges facing our nation, I urge my colleagues to also consider simple solutions to help working families make ends meet. We can help give more money to American consumers today without borrowing money that must be repaid tomorrow. Let's start by eliminating some of the worst abuses in lending by establishing a reasonable fee and interest rate cap.

I urge my colleagues to support the Protecting Consumers from Unreasonable Credit Rates Act.

Mr. President, I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the text of the bill was ordered to be printed in the RECORD, as follows:

S. 3452

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Protecting Consumers from Unreasonable Credit Rates Act of 2012''.

SEC. 2. FINDINGS.

Congress finds that—

(1) attempts have been made to prohibit usurious interest rates in America since colonial times;

(2) at the Federal level, in 2006, Congress enacted a Federal 36 percent annualized usury cap for service members and their families for covered credit products, as defined by the Department of Defense, which curbed payday, car title, and tax refund lending around military bases;

(3) notwithstanding such attempts to curb predatory lending, high-cost lending persists in all 50 States due to loopholes in State laws, safe harbor laws for specific forms of credit, and the exportation of unregulated interest rates permitted by preemption;

(4) due to the lack of a comprehensive Federal usury cap, consumers annually pay approximately $23,700,000,000 for high-cost overdraft loans, as much as $8,100,000,000 for storefront and online payday loans, and additional amounts in unreported revenues from bank direct deposit advance loans and high-cost online installment loans;

(5) cash-strapped consumers pay on average 400 percent annual interest for payday loans, 300 percent annual interest for car title loans, up to 3,500 percent for bank overdraft loans, and triple-digit rates for online installment loans;

(6) a national maximum interest rate that includes all forms of fees and closes all loopholes is necessary to eliminate such predatory lending; and

(7) alternatives to predatory lending that encourage small dollar loans with minimal or no fees, installment payment schedules, and affordable repayment periods should be encouraged.

SEC. 3. NATIONAL MAXIMUM INTEREST RATE.

The Truth in Lending Act (15 U.S.C. 1601 et seq.) is amended by adding at the end the following:

''SEC. 141. MAXIMUM RATES OF INTEREST.

''(a) IN GENERAL.—Notwithstanding any other provision of law, no creditor may make an extension of credit to a consumer with respect to which the fee and interest rate, as defined in subsection (b), exceeds 36 percent.

''(b) FEE AND INTEREST RATE DEFINED.—

''(1) IN GENERAL.—For purposes of this section, the fee and interest rate includes all charges payable, directly or indirectly, incident to, ancillary to, or as a condition of the extension of credit, including—

''(A) any payment compensating a creditor or prospective creditor for—

''(i) an extension of credit or making available a line of credit, such as fees connected with credit extension or availability such as numerical periodic rates, annual fees, cash advance fees, and membership fees; or

''(ii) any fees for default or breach by a borrower of a condition upon which credit was extended, such as late fees, creditor-imposed not sufficient funds fees charged when a borrower tenders payment on a debt with a check drawn on insufficient funds, overdraft fees, and over limit fees;

''(B) all fees which constitute a finance charge, as defined by rules of the Bureau in accordance with this title;

''(C) credit insurance premiums, whether optional or required; and

''(D) all charges and costs for ancillary products sold in connection with or incidental to the credit transaction.

''(2) TOLERANCES.—

''(A) IN GENERAL.—With respect to a credit obligation that is payable in at least 3 fully amortizing installments over at least 90 days, the term 'fee and interest rate' does not include—

''(i) application or participation fees that in total do not exceed the greater of $30 or, if there is a limit to the credit line, 5 percent of the credit limit, up to $120, if—

''(I) such fees are excludable from the finance charge pursuant to section 106 and regulations issued thereunder;

''(II) such fees cover all credit extended or renewed by the creditor for 12 months; and

''(III) the minimum amount of credit extended or available on a credit line is equal to $300 or more;

''(ii) a late fee charged as authorized by State law and by the agreement that does not exceed either $20 per late payment or $20 per month; or

''(iii) a creditor-imposed not sufficient funds fee charged when a borrower tenders payment on a debt with a check drawn on insufficient funds that does not exceed $15.

''(B) ADJUSTMENTS FOR INFLATION.—The Bureau may adjust the amounts of the tolerances established under this paragraph for inflation over time, consistent with the primary goals of protecting consumers and ensuring that the 36 percent fee and interest rate limitation is not circumvented.

''(c) CALCULATIONS.—

''(1) OPEN END CREDIT PLANS.—For an open end credit plan—

''(A) the fee and interest rate shall be calculated each month, based upon the sum of

all fees and finance charges described in subsection (b) charged by the creditor during the preceding 1-year period, divided by the average daily balance; and

''(B) if the credit account has been open less than 1 year, the fee and interest rate shall be calculated based upon the total of all fees and finance charges described in subsection (b)(1) charged by the creditor since the plan was opened, divided by the average daily balance, and multiplied by the quotient of 12 divided by the number of full months that the credit plan has been in existence.

''(2) OTHER CREDIT PLANS.—For purposes of this section, in calculating the fee and interest rate, the Bureau shall require the method of calculation of annual percentage rate specified in section 107(a)(1), except that the amount referred to in that section 107(a)(1) as the 'finance charge' shall include all fees, charges, and payments described in subsection (b)(1) of this section.

''(3) ADJUSTMENTS AUTHORIZED.—The Bureau may make adjustments to the calculations in paragraphs (1) and (2), but the primary goals of such adjustment shall be to protect consumers and to ensure that the 36 percent fee and interest rate limitation is not circumvented.

''(d) DEFINITION OF CREDITOR.—As used in this section, the term 'creditor' has the same meaning as in section 702(e) of the Equal Credit Opportunity Act (15 U.S.C. 1691a(e)).

''(e) NO EXEMPTIONS PERMITTED.—The exemption authority of the Bureau under section 105 shall not apply to the rates established under this section or the disclosure requirements under section 127(b)(6).

''(f) DISCLOSURE OF FEE AND INTEREST RATE FOR CREDIT OTHER THAN OPEN END CREDIT PLANS.—In addition to the disclosure requirements under section 127(b)(6), the Bureau may prescribe regulations requiring disclosure of the fee and interest rate established under this section.

''(g) RELATION TO STATE LAW.—Nothing in this section may be construed to preempt any provision of State law that provides greater protection to consumers than is provided in this section.

''(h) CIVIL LIABILITY AND ENFORCEMENT.—In addition to remedies available to the consumer under section 130(a), any payment compensating a creditor or prospective creditor, to the extent that such payment is a transaction made in violation of this section, shall be null and void, and not enforceable by any party in any court or alternative dispute resolution forum, and the creditor or any subsequent holder of the obligation shall promptly return to the consumer any principal, interest, charges, and fees, and any security interest associated with such transaction. Notwithstanding any statute of limitations or repose, a violation of this section may be raised as a matter of defense by recoupment or setoff to an action to collect such debt or repossess related security at any time.

''(i) VIOLATIONS.—Any person that violates this section, or seeks to enforce an agreement made in violation of this section, shall be subject to, for each such violation, 1 year in prison and a fine in an amount equal to the greater of—

''(1) 3 times the amount of the total accrued debt associated with the subject transaction; or

''(2) $50,000.

''(j) STATE ATTORNEYS GENERAL.—An action to enforce this section may be brought by the appropriate State attorney general in any United States district court or any other court of competent jurisdiction within 3 years from the date of the violation, and such attorney general may obtain injunctive relief.''.

SEC. 4. DISCLOSURE OF FEE AND INTEREST RATE FOR OPEN END CREDIT PLANS.

Section 127(b)(6) of the Truth in Lending Act (15 U.S.C. 1637(b)(6)) is amended by striking ''the total finance charge expressed'' and all that follows through the end of the paragraph and inserting ''the fee and interest rate, displayed as 'FAIR', established under section 141.''.

By Mr. HARKIN (for himself, Ms. MIKULSKI, Mrs. MURRAY, Mr. SANDERS, Mr. MERKLEY, Mr. FRANKEN, Mr. BLUMENTHAL, Mr. LEAHY, Mr. AKAKA, Mrs. BOXER, Mr. WYDEN, Mr. DURBIN, Mr. SCHUMER, Mr. LAUTENBERG, Mr. BROWN of Ohio, and Mrs. GILLIBRAND);

S. 3453. A bill to provide for an increase in the Federal minimum wage; to the Committee on Health, Education, Labor, and Pensions.

Mr. HARKIN. Mr. President, I have come to the floor many times over the past couple of years to talk about the decline of the American Dream. The American Dream is supposed to be about building a better life. If you work hard and play by the rules, you should be able to support your family, join the middle class, and provide a brighter future for your children. Unfortunately, this dream is nothing more than an illusion for millions of hardworking people who are trying to get by working in low-wage jobs. They are working hard and playing by the rules, but they face declining wages, declining opportunities, and declining economic security. Even working full-time, all year round, they can't make ends meet, much less join the middle class. That is not what America is supposed to be about.

That is why today I am introducing legislation that has one of the simplest and most effective policy solutions for shoring up the wages and financial security of our nation's low-wage workers. My bill, the Fair Minimum Wage Act of 2012, will raise the minimum wage. I would like to recognize my colleague in the House of Representatives, Ranking Member on the Education and Workforce Committee, GEORGE MILLER, who is joining me in this effort.

My bill will do three things: First, it will raise the minimum wage to $9.80 per hour in three steps over the course of 2 years. Second, it will link the minimum wage in the future to increases in the cost of living, through the Consumer Price Index, so that low-wage workers no longer fall further and further behind. Third, for the first time in more than 20 years, it will raise the minimum wage lags for tipped workers, from a paltry $2.13 per hour to a level that is 70 percent of the full minimum wage, or around $6.85 per hour. This will be a gradual change, accomplished over 5 years, that will give businesses time to adjust while providing more fairness for hardworking people who work in tipped industries.

This bill and these raises are long overdue. We all know that working Americans' paychecks have been stagnant for decades. But the situation is even worse for minimum wage workers. Today the minimum wage lags far behind its historic levels. It hasn't kept up with any other indicator in our economy, not with costs, or average wages, or our still rapid growth in productivity.

At its peak value in 1968, the minimum wage was worth more than $10.50 in today's dollars. That means that the minimum wage has lost 31 percent of its buying power since the late 1960s. How can we possibly allow this to be? Costs have been rising in real terms, on everything from food and rent to big-ticket items like health care and a college education. But Congress has let the minimum wage languish. The lowest wage workers in our society simply cannot afford this.

Even if we measured the minimum wage against other indicators in our economy, it has not kept up. The minimum wage used to be more than half of average wages; now it is barely a third. In the 1960s and 1970s, the minimum wage kept a family of three above the poverty line, 20 percent above it in 1968. But today, the minimum wage lags behind the poverty line by 16 percent. And let's not forget that the poverty line is a woefully inadequate measure of what families really need by any realistic measure. Who in this chamber could support two children on $18,000 per year, which is the official poverty line? Yet the minimum wage only pays $15,000 a year to someone working full-time who never takes a single day off all year. My bill will raise the minimum wage to about $20,000 per year, and it will maintain the wage at a level that keeps up with rising costs.

While workers are working longer and harder than ever, their paychecks don't reflect that contribution. If the minimum wage had kept up with productivity growth since 1968, it would be nearly $22 an hour this year; even if it had kept up with just one-quarter of productivity growth, it would be $12.25 per hour. So while companies have reaped the benefits of all this productivity growth, the people who actually do the work have seen none of its value. It has all gone to executive management and shareholders. It has gone to profits, not the people who do the work.

There will be tens of millions of people in this country who will benefit from this legislation. Twenty-eight million workers will get a raise, either directly by the legislation, or indirectly through the ''trickle up'' effects of a higher wage floor—that is more than a fifth of our workforce that will be impacted. Among them, more than half are women, and more than four in ten are people of color—both of these groups are overrepresented in low-wage work. They are the ones who care for our children and elders, who clean our offices and factories, who serve us food, who keep our economic engine running. These are some of the hardest jobs and

hardest workers, and yet their pay is simply paltry. We will never have fair wages for women or greater racial equality if the minimum wage is not a just and fair minimum wage.

The families of these 28 million workers will also benefit. More than 21 million children have parents who will get a raise. This will be so meaningful to these families. After all, children represent more than a third of poor Americans. Nearly half of children, 44 percent, are poor or low-income, and even among families with parents working full-time year-round, nearly three in ten children are poor or low-income. This is largely because wages are much too low to support a family.

Yet wages aren't low because our economy can't afford them. No. Our economic growth is going to profits, not to workers. Inequality is at the highest level we've seen since the eve of the Great Depression. CEOs are raking in millions—even if their companies are not performing well—while low-wage workers are barely able to put food on the table, and even then it is often with the help of food stamps. Last year, the average CEO earned nearly $13 million. That was after a 23 percent raise in 2010 and a 14 percent raise in 2011. Minimum wage workers had no raises in those years. But CEOs are getting $13 million a year. That is more than $6,200 an hour. A CEO earns more before lunch on his first day of work than a minimum wage worker earns in an entire year.

Some people will criticize this measure, saying it will force businesses to lay off workers, and that workers will actually be hurt by getting a raise. History proves that these assertions are simply wrong. We know from decades of rigorous research that minimum wage raises along the lines of what I am proposing do not have negative jobs effects—and if there are any effects on jobs, they are small, but positive effects. This goes for teenagers, too; study after study confirms minimum wage raises do not cause teenage unemployment.

Indeed, businesses are helped when their workers get a raise because raising the minimum wage acts like a stimulus. Businesses will reap more in sales when their customers have more money in their pockets, and they will save money through increased productivity and morale and reduced turnover. My bill will put an extra $40 billion in the hands of low-wage workers and their families. We know that these workers don't have much if any room for savings—they will go out and spend it, and this will benefit the local businesses in their communities. Indeed, this extra spending power will boost GDP by more than $25 billion and add 100,000 jobs, as increased economic activity ripples through the economy.

Businesses will also save from reduced turnover cost, since turnover rates fall when workers earn more money. It can cost thousands of dollars to recruit, hire, and train new employees, even for low-skill jobs. Of course all businesses would have the same minimum wage, meaning no business would be any worse off than a competitor. A raise in the minimum wage would also reduce competitive disadvantage faced by businesses that already pay a higher wage. These businesses should be rewarded, not punished for paying fair wages.

We must also look at what is happening in our economy. We are becoming a low-wage economy. Low-wage jobs are growing faster than middle- or high-wage jobs. Over the next decade, the Bureau of Labor Statistics estimates that 7 of the 10 occupations with the largest job growth will be low-wage jobs. With so much of our economy moving to the low end of the wage scale, we must ensure that those wages are adequate.

It is long past time to establish a fair minimum wage in our country. It is good for families, good for business and good for our economy. Most importantly, it is the right thing to do. People who work hard for a living should not have to live in poverty. I am proud to introduce this bill today, to raise the minimum wage, and to help tens of millions of workers and their families.

Mr. President, I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the text of the bill was ordered to be printed in the RECORD. as follows:

S. 3453

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Fair Minimum Wage Act of 2012''.

SEC. 2. MINIMUM WAGE INCREASES.

(a) MINIMUM WAGE.—

(1) IN GENERAL.—Section 6(a)(1) of the Fair Labor Standards Act of 1938 (29 U.S.C. 206(a)(1)) is amended to read as follows:

''(1) except as otherwise provided in this section, not less than—

''(A) $8.10 an hour, beginning on the first day of the third month that begins after the date of enactment of the Fair Minimum Wage Act of 2012 Act;

''(B) $8.95 an hour, beginning 1 year after that first day;

''(C) $9.80 an hour, beginning 2 years after that first day; and

''(D) beginning on the date that is 3 years after that first day, and annually thereafter, the amount determined by the Secretary pursuant to subsection (h);''.

(2) DETERMINATION BASED ON INCREASE IN THE CONSUMER PRICE INDEX.—Section 6 of the Fair Labor Standards Act of 1938 (29 U.S.C. 206) is amended by adding at the end the following:

''(h)(1) Each year, by not later than the date that is 90 days before a new minimum wage determined under subsection (a)(1)(D) is to take effect, the Secretary shall determine the minimum wage to be in effect pursuant to this subsection for the subsequent 1-year period. The wage determined pursuant to this subsection for a year shall be—

''(A) not less than the amount in effect under subsection (a)(1) on the date of such determination;

''(B) increased from such amount by the annual percentage increase in the Consumer Price Index for Urban Wage Earners and Clerical Workers (United States city average, all items, not seasonally adjusted), or its successor publication, as determined by the Bureau of Labor Statistics; and

''(C) rounded to the nearest multiple of $0.05.

''(2) In calculating the annual percentage increase in the Consumer Price Index for purposes of paragraph (1)(B), the Secretary shall compare such Consumer Price Index for the most recent month, quarter, or year available (as selected by the Secretary prior to the first year for which a minimum wage is in effect pursuant to this subsection) with the Consumer Price Index for the same month in the preceding year, the same quarter in the preceding year, or the preceding year, respectively.''.

(b) BASE MINIMUM WAGE FOR TIPPED EMPLOYEES.—Section 3(m)(1) of the Fair Labor Standards Act of 1938 (29 U.S.C. 203(m)(1)) is amended to read as follows:

''(1) the cash wage paid such employee, which for purposes of such determination shall be not less than—

''(A) for the 1-year period beginning on the first day of the third month that begins after the date of enactment of the Fair Minimum Wage Act of 2012, $3.00 an hour;

''(B) for each succeeding 1-year period until the hourly wage under this paragraph equals 70 percent of the wage in effect under section 6(a)(1) for such period, an hourly wage equal to the amount determined under this paragraph for the preceding year, increased by the lesser of—

''(i) $0.85; or

''(ii) the amount necessary for the wage in effect under this paragraph to equal 70 percent of the wage in effect under section 6(a)(1) for such period, rounded to the nearest multiple of $0.05; and

''(C) for each succeeding 1-year period after the year in which the hourly wage under this paragraph first equals 70 percent of the wage in effect under section 6(a)(1) for the same period, the amount necessary to ensure that the wage in effect under this paragraph remains equal to 70 percent of the wage in effect under section 6(a)(1), rounded to the nearest multiple of $0.05; and''.

(c) PUBLICATION OF NOTICE.—Section 6 of the Fair Labor Standards Act of 1938 (as amended by subsection (a)) (29 U.S.C. 206) is further amended by adding at the end the following:

''(i) Not later than 60 days prior to the effective date of any increase in the minimum wage determined under subsection (h) or required for tipped employees in accordance with subparagraph (B) or (C) of section 3(m)(1), as amended by the Fair Minimum Wage Act of 2012, the Secretary shall publish in the Federal Register and on the website of the Department of Labor a notice announcing the adjusted required wage.''.

(d) EFFECTIVE DATE.—The amendments made by subsections (a) and (b) shall take effect on the first day of the third month that begins after the date of enactment of this Act.

SUBMITTED RESOLUTIONS

SENATE RESOLUTION 529—RECOGNIZING THAT THE OCCURRENCE OF PROSTATE CANCER IN AFRICAN-AMERICAN MEN HAS REACHED EPIDEMIC PROPORTIONS AND URGING FEDERAL AGENCIES TO ADDRESS THAT HEALTH CRISIS BY SUPPORTING EDUCATION, AWARENESS OUTREACH, AND RESEARCH SPECIFICALLY FOCUSED ON HOW PROSTATE CANCER AFFECTS AFRICAN-AMERICAN MEN

Mr. KERRY (for himself, Mr. CHAMBLISS, Mr. INOUYE, Mr. WYDEN, Mr. AKAKA, and Mr. CARDIN) submitted the following resolution; which was considered and agreed to:

S. RES. 529

Whereas the incidence of prostate cancer in African-American men is more than one and a half times higher than in any other racial or ethnic group in the United States;

Whereas African-American men have the highest mortality rate of any ethnic and racial group in the United States, dying at a rate that is approximately two and a half times higher than other ethnic and racial groups;

Whereas that rate of mortality represents the largest disparity of mortality rates in any of the major cancers;

Whereas prostate cancer can be cured with early detection and the proper treatment, regardless of the ethnic or racial group of the cancer patient;

Whereas African Americans are more likely to be diagnosed at an earlier age and at a later stage of cancer progression than all other ethnic and racial groups, leading to lower cure rates and lower chances of survival;

Whereas, for patients diagnosed early, studies show a 5-year survival rate of nearly 100 percent, but the survival rate drops significantly to 28 percent for patients diagnosed in late stages; and

Whereas recent genomics research has increased the ability to identify men at high risk for aggressive prostate cancer: Now, therefore, be it

Resolved, That the Senate—

(1) recognizes that prostate cancer has created a health crisis for African-American men;

(2) recognizes the importance of health coverage and access to care, as well as promoting informed decisionmaking between men and their doctors, taking into consideration the known risks and potential benefits of screening and treatment options for prostate cancer;

(3) urges Federal agencies to support—

(A) research to address and attempt to end the health crisis created by prostate cancer;

(B) efforts relating to education, awareness, and early detection at the grassroots level to end that health crisis; and

(C) the Office of Minority Health of the Department of Health and Human Services in focusing on improving health and healthcare outcomes for African Americans at an elevated risk of prostate cancer; and

(4) urges investment by Federal agencies in research focusing on the improvement of early detection and treatment of prostate cancer, such as the use of—

(A) biomarkers to accurately distinguish indolent forms of prostate cancer from lethal forms; and

(B) advanced imaging tools to ensure the best level of individualized patient care.

SENATE RESOLUTION 530—DESIGNATING THE MONTH OF AUGUST 2012 AS ''NATIONAL REGISTERED APPRENTICESHIP MONTH''

Mrs. MURRAY (for herself, Mr. HARKIN, Mr. JOHNSON of Wisconsin, Mr. KOHL, Mr. BLUMENTHAL, Mr. PRYOR, and Ms. CANTWELL) submitted the following resolution; which was considered and agreed to:

S. RES. 530

Whereas 2012 marks the 75th anniversary of the enactment of the Act of August 16, 1937 (29 U.S.C. 50 et seq.) (commonly known as the ''National Apprenticeship Act''), which established the national registered apprenticeship system;

Whereas the State of Wisconsin created the first State registered apprenticeship system in 1911;

Whereas the Act of August 16, 1937 (29 U.S.C. 50 et seq.) (commonly known as the ''National Apprenticeship Act'') established a comprehensive system of partnerships among employers, labor organizations, educational institutions, and Federal and State governments, which has shaped skill training for succeeding generations of United States workers;

Whereas for 75 years, the national registered apprenticeship system has provided state of the art training using an model known as ''earn while you learn'' that offers a pathway to the middle class and a sustainable career for millions of workers in the United States;

Whereas the national registered apprenticeship system has grown to include approximately 24,000 programs across the United States, providing education and training for apprentices in emerging and high-growth sectors, such as information technology and health care, as well as in traditional industries;

Whereas the national registered apprenticeship system leverages approximately $1,000,000,000 in private investment, reflecting the strong commitment of the sponsors of the system, which include industry associations, individual employers, and labor-management partnerships;

Whereas the national registered apprenticeship system is an important post-secondary pathway for United States workers, offering a combination of academic and technical instruction with paid, on-the-job training, resulting in a nationally and industry-recognized occupational credential that ensures higher earnings for apprentices and a highly skilled workforce for United States businesses;

Whereas the national registered apprenticeship system has continually modernized and developed innovative training approaches to meet the workforce needs of industry and address the evolving challenges of staying competitive in the global economy;

Whereas the national registered apprenticeship system of the 21st century, as envisioned by the Advisory Committee on Apprenticeship of the Secretary of Labor and administered as a partnership between the Federal Government and State apprenticeship programs, is positioned to produce the highly skilled workers the United States economy needs now and in the future; and

Whereas the celebration of National Registered Apprenticeship Month—

(1) honors the industries that use the registered apprenticeship model;

(2) encourages other industries that could benefit from the registered apprenticeship model to train United States workers using the model; and

(3) recognizes the role the national registered apprenticeship system has played in preparing United States workers for jobs with family-sustaining wages: Now, therefore, be it

Resolved, That the Senate—

(1) designates August 2012, as ''National Registered Apprenticeship Month'';

(2) celebrates the 101st anniversary of the enactment of the first State registered apprenticeship law; and

(3) celebrates the 75th anniversary of the enactment of the Act of August 16, 1937 (29 U.S.C. 50 et seq.) (commonly known as the ''National Apprenticeship Act'').

SENATE RESOLUTION 531—COMMEMORATING THE SUCCESS OF TEAM USA IN THE PAST 25 OLYMPIC GAMES AND SUPPORTING TEAM USA IN THE 2012 OLYMPIC AND PARALYMPIC GAMES

Ms. KLOBUCHAR (for herself, Mr. HATCH, Mr. BENNET, Mr. ISAKSON, Mr. DURBIN, and Mr. MERKLEY) submitted the following resolution; which was considered and agreed to:

S. RES. 531

Whereas, for over 100 years, the Olympic Movement has built a more peaceful and better world by educating young people through amateur athletics, bringing together athletes from many countries in friendly competition, and forging new relationships bound by friendship, solidarity, and fair play;

Whereas the 2012 Olympic Games will take place in London, England from July 27, 2012 to August 12, 2012, and the 2012 Paralympic Games will take place from August 29, 2012 to September 9, 2012;

Whereas, at the 2012 Olympic Games, over 200 nations will compete in over 300 events, and Team USA will compete in 246 events;

Whereas, at the 2012 Olympic Games, over 200 nations will compete in 39 disciplines, and Team USA will compete in 38 of those disciplines;

Whereas 529 Olympians and over 245 Paralympians will compete on behalf of Team USA in London, England;

Whereas Team USA has won 934 gold medals, 730 silver medals, and 643 bronze medals, totaling 2,307 medals over the past 25 Olympic Games;

Whereas the people of the United States stand united in respect and admiration for the members of the United States Olympic and Paralympic teams, and the athletic accomplishments, sportsmanship, and dedication to excellence of the teams;

Whereas the many accomplishments of the United States Olympic and Paralympic teams would not have been possible without the hard work and dedication of many others, including the United States Olympic Committee and the many administrators, coaches, and family members who provided critical support to the athletes;

Whereas the Nation takes great pride in the qualities of commitment to excellence, grace under pressure, and good will toward other competitors exhibited by the athletes of Team USA; and

Whereas the Olympic Movement celebrates competition, fair play, and the pursuit of dreams: Now, therefore, be it

Resolved, That the Senate—

(1) applauds all of the athletes and coaches of Team USA and their families who support them;

(2) supports the athletes of Team USA in their endeavors at the 2012 Olympic and Paralympic Games held in London, England;

(3) thanks all of the members of the United States Olympics Committee for their unwavering support of the athletes of Team USA; and

(4) supports the goals and ideals of the Olympic Games.

SENATE RESOLUTION 532—EXPRESSING SUPPORT FOR THE XIX INTERNATIONAL AIDS CONFERENCE AND THE SENSE OF THE SENATE THAT CONTINUED COMMITMENT BY THE UNITED STATES TO HIV/AIDS RESEARCH, PREVENTION, AND TREATMENT PROGRAMS IS CRUCIAL TO PROTECTING GLOBAL HEALTH

Mr. NELSON of Florida (for himself, Mr. RUBIO, Mr. DURBIN, Mr. LEAHY, Ms. CANTWELL, Mr. LAUTENBERG, Mr. SESSIONS, Mr. ENZI, Mr. CARDIN, Ms. MIKULSKI, Ms. LANDRIEU, and Mr. KOHL) submitted the following resolution; which was considered and agreed to:

S. RES. 532

Whereas, according to UNAIDS, the Joint United Nations Programme on HIV/AIDS, there are approximately 33,400,000 people living with HIV worldwide, and nearly 30,000,000 people have died of AIDS since the first cases were reported in 1981;

Whereas, in the United States, more than 1,000,000 people are living with HIV and approximately 50,000 people become newly infected with the virus each year;

Whereas, according to the Centers for Disease Control and Prevention, 1 in 5 individuals living with HIV is unaware of the infection, underscoring the need for greater education about HIV/AIDS and access to testing;

Whereas societal stigma remains a significant challenge to addressing HIV/AIDS;

Whereas the United States is heavily engaged in both international and domestic efforts to address the HIV/AIDS pandemic, including—

(1) the United States President's Emergency Plan for AIDS Relief (commonly known as ''PEPFAR'');

(2) the Global Fund to Fight AIDS, Tuberculosis, and Malaria;

(3) title XXIV of the Public Health Service Act (42 U.S.C. 300dd et seq.) (originally enacted as part of the Ryan White Comprehensive AIDS Resources Emergency Act of 1990 (Public Law 101-381; 104 Stat. 576));

(4) State AIDS Drug Assistance Programs;

(5) the Housing Opportunities for Persons with AIDS program of the Department of Housing and Urban Development; and

(6) AIDS research at the National Institutes of Health and other agencies;

Whereas, since 1985, the now biennial International AIDS Conference has brought together leading scientists, public health experts, policymakers, community leaders, and individuals living with HIV/AIDS from around the world to enhance the global response to HIV/AIDS, evaluate recent scientific developments, share knowledge, and facilitate a collective strategy to combat the HIV/AIDS pandemic;

Whereas, in 2008, Congress passed and the President signed into law the Tom Lantos and Henry J. Hyde United States Global Leadership Against HIV/AIDS, Tuberculosis, and Malaria Reauthorization Act of 2008 (Public Law 110-293; 122 Stat. 2918);

Whereas taxpayers in the United States have paid more than $45,000,000,000 through PEPFAR and the Global Fund to Fight AIDS, Tuberculosis, and Malaria, which have enjoyed broad bipartisan support in Congress;

Whereas, 25 years after the III International AIDS Conference was held in Washington, D.C., the XIX International AIDS Conference (referred to in this preamble as ''AIDS 2012'') will take place from July 22, 2012, through July 27, 2012, at the Walter E. Washington Convention Center, in Washington, D.C.;

Whereas AIDS 2012, organized by the International AIDS Society, is expected to convene more than 20,000 delegates, including 2,000 journalists, from nearly 200 countries;

Whereas the theme of AIDS 2012, ''Turning the Tide Together'', embodies the promise and urgency of utilizing recent scientific advances in HIV/AIDS treatment and biomedical prevention, continuing research for an HIV vaccine and cure, and increasing effective, evidence-based interventions in key settings to change the course of the HIV/AIDS crisis;

Whereas AIDS 2012 seeks to engage governments, nongovernmental organizations, policymakers, the scientific community, the private sector, civil society, faith-based organizations, the media, and people living with HIV/AIDS to more effectively address regional, national, and local responses to HIV/AIDS around the world and overcome barriers that limit access to preventative care, treatment, and other services; and

Whereas AIDS 2012 is a tremendous opportunity to strengthen the role of the United States in global HIV/AIDS initiatives within the context of significant global economic challenges, reenergize the response to the domestic epidemic, and focus particular attention on the devastating impact of HIV/AIDS that continues in the United States: Now, therefore, be it

Resolved, That the Senate—

(1) supports the XIX International AIDS Conference and the goal of renewing awareness of, and commitment to, addressing the HIV/AIDS crisis in the United States and abroad;

(2) recognizes that continued HIV/AIDS research, prevention, and treatment programs are crucial to improving global health;

(3) understands that the key to overcoming HIV/AIDS includes efforts to formulate sound public health policy, protect human rights, address the needs of women and girls, direct effective programming toward the populations at the highest risk of infection, ensure accountability, and combat stigma, poverty, and other social challenges related to HIV/AIDS;

(4) seeks to work with all stakeholders—

(A) to prevent the transmission of HIV;

(B) to increase access to testing, treatment, and care;

(C) to improve health outcomes for all people living with HIV/AIDS; and

(D) to foster greater scientific and programmatic collaborations around the world to translate scientific advances and apply best practices to international efforts to end HIV/AIDS;

(5) commits to supporting a stronger global response to HIV/AIDS, protecting the rights of people living with HIV/AIDS, and working to create an ''AIDS-free generation''; and

(6) encourages the ongoing development in the public and private sectors of innovative therapies and advances in clinical treatment for HIV/AIDS, including—

(A) new and improved biomedical and behavioral prevention strategies;

(B) safer and more affordable, accessible, and effective treatment regimens for infected individuals; and

(C) research for an HIV vaccine and cure.

AMENDMENTS SUBMITTED AND PROPOSED

SA 2581. Mrs. HUTCHISON (for herself, Mr. MCCAIN, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin) submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table.

SA 2582. Mrs. HUTCHISON (for herself, Mr. MCCAIN, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin) submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2583. Mr. GRASSLEY submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2584. Mr. GRASSLEY submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2585. Mr. GRASSLEY submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2586. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2587. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2588. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2589. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2590. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2591. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2592. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2593. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2594. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2595. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2596. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2597. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2598. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2599. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2600. Mr. MCCAIN submitted an amendment intended to be proposed by him to the

bill S. 3414, supra; which was ordered to lie on the table.

SA 2601. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2602. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2603. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2604. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2605. Mr. MCCAIN (for himself, Mrs. HUTCHISON, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2606. Mr. MCCAIN (for himself, Mrs. HUTCHISON, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2607. Mr. MCCAIN (for himself, Mrs. HUTCHISON, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2608. Mr. MCCAIN (for himself, Mrs. HUTCHISON, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2609. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2610. Mrs. HUTCHISON submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2611. Mrs. HUTCHISON submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2612. Mrs. HUTCHISON submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2613. Mrs. HUTCHISON (for herself, Mr. MCCAIN, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin) submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2614. Mrs. HUTCHISON (for herself, Mr. MCCAIN, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin) submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2615. Mrs. HUTCHISON submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2616. Mrs. SHAHEEN (for herself and Mr. PORTMAN) submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2617. Mr. COONS (for himself, Mr. WYDEN, Mr. AKAKA, Mr. FRANKEN, Mr. UDALL of New Mexico, and Mr. SANDERS) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2618. Mr. AKAKA (for himself, Mr. BLUMENTHAL, Mr. COONS, Mr. FRANKEN, Mr. SANDERS, Mr. UDALL of New Mexico, and Mr. WYDEN) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2619. Mr. DEMINT submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2620. Mr. HOEVEN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

TEXT OF AMENDMENTS

SA 2581. Mrs. HUTCHISON (for herself, Mr. MCCAIN, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin) submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012'' or ''SECURE IT''.

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

TITLE I—FACILITATING SHARING OF CYBER THREAT INFORMATION

SEC. 101. DEFINITIONS.

In this title:

(1) AGENCY.—The term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code.

(2) ANTITRUST LAWS.—The term ''antitrust laws''—

(A) has the meaning given the term in section 1(a) of the Clayton Act (15 U.S.C. 12(a));

(B) includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that section 5 of that Act applies to unfair methods of competition; and

(C) includes any State law that has the same intent and effect as the laws under subparagraphs (A) and (B).

(3) COUNTERMEASURE.—The term ''countermeasure'' means an automated or a manual action with defensive intent to mitigate cyber threats.

(4) CYBER THREAT INFORMATION.—The term ''cyber threat information'' means information that indicates or describes—

(A) a technical or operation vulnerability or a cyber threat mitigation measure;

(B) an action or operation to mitigate a cyber threat;

(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

(D) a method of defeating a technical control;

(E) a method of defeating an operational control;

(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

(G) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to inadvertently enable the defeat of a technical or operational control;

(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

(J) any combination of subparagraphs (A) through (I).

(5) CYBERSECURITY CENTER.—The term ''cybersecurity center'' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint

Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

(6) CYBERSECURITY SYSTEM.—The term ''cybersecurity system'' means a system designed or employed to ensure the integrity, confidentiality, or availability of, or to safeguard, a system or network, including measures intended to protect a system or network from—

(A) efforts to degrade, disrupt, or destroy such system or network; or

(B) theft or misappropriations of private or government information, intellectual property, or personally identifiable information.

(7) ENTITY.—

(A) IN GENERAL.—The term ''entity'' means any private entity, non-Federal government agency or department, or State, tribal, or local government agency or department (including an officer, employee, or agent thereof).

(B) INCLUSIONS.—The term ''entity'' includes a government agency or department (including an officer, employee, or agent thereof) of the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States.

(8) FEDERAL INFORMATION SYSTEM.—The term ''Federal information system'' means an information system of a Federal department or agency used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

(9) INFORMATION SECURITY.—The term ''information security'' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; or

(C) availability, by ensuring timely and reliable access to and use of information.

(10) INFORMATION SYSTEM.—The term ''information system'' has the meaning given the term in section 3502 of title 44, United States Code.

(11) LOCAL GOVERNMENT.—The term ''local government'' means any borough, city, county, parish, town, township, village, or other general purpose political subdivision of a State.

(12) MALICIOUS RECONNAISSANCE.—The term ''malicious reconnaissance'' means a method for actively probing or passively monitoring an information system for the purpose of discerning technical vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(13) OPERATIONAL CONTROL.—The term ''operational control'' means a security control for an information system that primarily is implemented and executed by people.

(14) OPERATIONAL VULNERABILITY.—The term ''operational vulnerability'' means any attribute of policy, process, or procedure that could enable or facilitate the defeat of an operational control.

(15) PRIVATE ENTITY.—The term ''private entity'' means any individual or any private group, organization, or corporation, including an officer, employee, or agent thereof.

(16) SIGNIFICANT CYBER INCIDENT.—The term ''significant cyber incident'' means a cyber incident resulting in, or an attempted cyber incident that, if successful, would have resulted in—

(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

(17) TECHNICAL CONTROL.—The term ''technical control'' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

(18) TECHNICAL VULNERABILITY.—The term ''technical vulnerability'' means any attribute of hardware or software that could enable or facilitate the defeat of a technical control.

(19) TRIBAL.—The term ''tribal'' has the meaning given the term ''Indian tribe'' in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

SEC. 102. AUTHORIZATION TO SHARE CYBER THREAT INFORMATION.

(a) VOLUNTARY DISCLOSURE.—

(1) PRIVATE ENTITIES.—Notwithstanding any other provision of law, a private entity may, for the purpose of preventing, investigating, or otherwise mitigating threats to information security, on its own networks, or as authorized by another entity, on such entity's networks, employ countermeasures and use cybersecurity systems in order to obtain, identify, or otherwise possess cyber threat information.

(2) ENTITIES.—Notwithstanding any other provision of law, an entity may disclose cyber threat information to—

(A) a cybersecurity center; or

(B) any other entity in order to assist with preventing, investigating, or otherwise mitigating threats to information security.

(3) INFORMATION SECURITY PROVIDERS.—If the cyber threat information described in paragraph (1) is obtained, identified, or otherwise possessed in the course of providing information security products or services under contract to another entity, that entity shall be given, at any time prior to disclosure of such information, a reasonable opportunity to authorize or prevent such disclosure, to request anonymization of such information, or to request that reasonable efforts be made to safeguard such information that identifies specific persons from unauthorized access or disclosure.

(b) SIGNIFICANT CYBER INCIDENTS INVOLVING FEDERAL INFORMATION SYSTEMS.—

(1) IN GENERAL.—An entity providing electronic communication services, remote computing services, or information security services to a Federal department or agency shall inform the Federal department or agency of a significant cyber incident involving the Federal information system of that Federal department or agency that—

(A) is directly known to the entity as a result of providing such services;

(B) is directly related to the provision of such services by the entity; and

(C) as determined by the entity, has impeded or will impede the performance of a critical mission of the Federal department or agency.

(2) ADVANCE COORDINATION.—A Federal department or agency receiving the services described in paragraph (1) shall coordinate in advance with an entity described in paragraph (1) to develop the parameters of any information that may be provided under paragraph (1), including clarification of the type of significant cyber incident that will impede the performance of a critical mission of the Federal department or agency.

(3) REPORT.—A Federal department or agency shall report information provided under this subsection to a cybersecurity center.

(4) CONSTRUCTION.—Any information provided to a cybersecurity center under paragraph (3) shall be treated in the same manner as information provided to a cybersecurity center under subsection (a).

(c) INFORMATION SHARED WITH OR PROVIDED TO A CYBERSECURITY CENTER.—Cyber threat information provided to a cybersecurity center under this section—

(1) may be disclosed to, retained by, and used by, consistent with otherwise applicable Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal government for a cybersecurity purpose, a national security purpose, or in order to prevent, investigate, or prosecute any of the offenses listed in section 2516 of title 18, United States Code, and such information shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under this paragraph;

(2) may, with the prior written consent of the entity submitting such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(3) shall be considered the commercial, financial, or proprietary information of the entity providing such information to the Federal government and any disclosure outside the Federal government may only be made upon the prior written consent by such entity and shall not constitute a waiver of any applicable privilege or protection provided by law, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(4) shall be deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records;

(5) shall be, without discretion, withheld from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records;

(6) shall not be subject to the rules of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official;

(7) shall not, if subsequently provided to a State, tribal, or local government or government agency, otherwise be disclosed or distributed to any entity by such State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent; and

(8) shall not be directly used by any Federal, State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing

cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph.

(d) PROCEDURES RELATING TO INFORMATION SHARING WITH A CYBERSECURITY CENTER.—Not later than 60 days after the date of enactment of this Act, the heads of each department or agency containing a cybersecurity center shall jointly develop, promulgate, and submit to Congress procedures to ensure that cyber threat information shared with or provided to—

(1) a cybersecurity center under this section—

(A) may be submitted to a cybersecurity center by an entity, to the greatest extent possible, through a uniform, publicly available process or format that is easily accessible on the website of such cybersecurity center, and that includes the ability to provide relevant details about the cyber threat information and written consent to any subsequent disclosures authorized by this paragraph;

(B) shall immediately be further shared with each cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government;

(C) is handled by the Federal government in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title, and the Federal government may undertake efforts consistent with this subparagraph to limit the impact on privacy and civil liberties of the sharing of cyber threat information with the Federal government; and

(D) except as provided in this section, shall only be used, disclosed, or handled in accordance with the provisions of subsection (c); and

(2) a Federal agency or department under subsection (b) is provided immediately to a cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government.

(e) INFORMATION SHARED BETWEEN ENTITIES.—

(1) IN GENERAL.—An entity sharing cyber threat information with another entity under this title may restrict the use or sharing of such information by such other entity.

(2) FURTHER SHARING.—Cyber threat information shared by any entity with another entity under this title—

(A) shall only be further shared in accordance with any restrictions placed on the sharing of such information by the entity authorizing such sharing, such as appropriate anonymization of such information; and

(B) may not be used by any entity to gain an unfair competitive advantage to the detriment of the entity authorizing the sharing of such information, except that the conduct described in paragraph (3) shall not constitute unfair competitive conduct.

(3) INFORMATION SHARED WITH STATE, TRIBAL, OR LOCAL GOVERNMENT OR GOVERNMENT AGENCY.—Cyber threat information shared with a State, tribal, or local government or government agency under this title—

(A) may, with the prior written consent of the entity sharing such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent;

(B) shall be deemed voluntarily shared information and exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records;

(C) shall not be disclosed or distributed to any entity by the State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent; and

(D) shall not be directly used by any State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this subparagraph.

(4) ANTITRUST EXEMPTION.—The exchange or provision of cyber threat information or assistance between 2 or more private entities under this title shall not be considered a violation of any provision of antitrust laws if exchanged or provided in order to assist with—

(A) facilitating the prevention, investigation, or mitigation of threats to information security; or

(B) communicating or disclosing of cyber threat information to help prevent, investigate or otherwise mitigate the effects of a threat to information security.

(5) NO RIGHT OR BENEFIT.—The provision of cyber threat information to an entity under this section shall not create a right or a benefit to similar information by such entity or any other entity.

(f) FEDERAL PREEMPTION.—

(1) IN GENERAL.—This section supersedes any statute or other law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this section.

(2) STATE LAW ENFORCEMENT.—Nothing in this section shall be construed to supersede any statute or other law of a State or political subdivision of a State concerning the use of authorized law enforcement techniques.

(3) PUBLIC DISCLOSURE.—No information shared with or provided to a State, tribal, or local government or government agency pursuant to this section shall be made publicly available pursuant to any State, tribal, or local law requiring disclosure of information or records.

(g) CIVIL AND CRIMINAL LIABILITY.—

(1) GENERAL PROTECTIONS.—

(A) PRIVATE ENTITIES.—No cause of action shall lie or be maintained in any court against any private entity for—

(i) the use of countermeasures and cybersecurity systems as authorized by this title;

(ii) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(iii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such private entity.

(B) ENTITIES.—No cause of action shall lie or be maintained in any court against any entity for—

(i) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(ii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such entity.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed as creating any immunity against, or otherwise affecting, any action brought by the Federal government, or any agency or department thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, and use of classified information.

(h) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this section shall be construed to limit or prohibit otherwise lawful disclosures of communications, records, or other information by a private entity to any other governmental or private entity not covered under this section.

(i) WHISTLEBLOWER PROTECTION.—Nothing in this Act shall be construed to preempt or preclude any employee from exercising rights currently provided under any whistleblower law, rule, or regulation.

(j) RELATIONSHIP TO OTHER LAWS.—The submission of cyber threat information under this section to a cybersecurity center shall not affect any requirement under any other provision of law for an entity to provide information to the Federal government.

SEC. 103. INFORMATION SHARING BY THE FEDERAL GOVERNMENT.

(a) CLASSIFIED INFORMATION.—

(1) PROCEDURES.—Consistent with the protection of intelligence sources and methods, and as otherwise determined appropriate, the Director of National Intelligence and the Secretary of Defense, in consultation with the heads of the appropriate Federal departments or agencies, shall develop and promulgate procedures to facilitate and promote—

(A) the immediate sharing, through the cybersecurity centers, of classified cyber threat information in the possession of the Federal government with appropriately cleared representatives of any appropriate entity; and

(B) the declassification and immediate sharing, through the cybersecurity centers, with any entity or, if appropriate, public availability of cyber threat information in the possession of the Federal government;

(2) HANDLING OF CLASSIFIED INFORMATION.—The procedures developed under paragraph (1) shall ensure that each entity receiving classified cyber threat information pursuant to this section has acknowledged in writing the ongoing obligation to comply with all laws, executive orders, and procedures concerning the appropriate handling, disclosure, or use of classified information.

(b) UNCLASSIFIED CYBER THREAT INFORMATION.—The heads of each department or agency containing a cybersecurity center shall jointly develop and promulgate procedures that ensure that, consistent with the provisions of this section, unclassified, including controlled unclassified, cyber threat information in the possession of the Federal government—

(1) is shared, through the cybersecurity centers, in an immediate and adequate manner with appropriate entities; and

(2) if appropriate, is made publicly available.

(c) DEVELOPMENT OF PROCEDURES.—

(1) IN GENERAL.—The procedures developed under this section shall incorporate, to the greatest extent possible, existing processes utilized by sector specific information sharing and analysis centers.

(2) COORDINATION WITH ENTITIES.—In developing the procedures required under this section, the Director of National Intelligence and the heads of each department or agency containing a cybersecurity center shall coordinate with appropriate entities to ensure that protocols are implemented that will facilitate and promote the sharing of cyber threat information by the Federal government.

(d) ADDITIONAL RESPONSIBILITIES OF CYBERSECURITY CENTERS.—Consistent with section 102, a cybersecurity center shall—

(1) facilitate information sharing, interaction, and collaboration among and between cybersecurity centers and—

(A) other Federal entities;

(B) any entity; and

(C) international partners, in consultation with the Secretary of State;

(2) disseminate timely and actionable cybersecurity threat, vulnerability, mitigation, and warning information, including alerts, advisories, indicators, signatures, and mitigation and response measures, to improve the security and protection of information systems; and

(3) coordinate with other Federal entities, as appropriate, to integrate information from across the Federal government to provide situational awareness of the cybersecurity posture of the United States.

(e) SHARING WITHIN THE FEDERAL GOVERNMENT.—The heads of appropriate Federal departments and agencies shall ensure that cyber threat information in the possession of such Federal departments or agencies that relates to the prevention, investigation, or mitigation of threats to information security across the Federal government is shared effectively with the cybersecurity centers.

(f) SUBMISSION TO CONGRESS.—Not later than 60 days after the date of enactment of this Act, the Director of National Intelligence, in coordination with the appropriate head of a department or an agency containing a cybersecurity center, shall submit the procedures required by this section to Congress.

SEC. 104. CONSTRUCTION.

(a) INFORMATION SHARING RELATIONSHIPS.—Nothing in this title shall be construed—

(1) to limit or modify an existing information sharing relationship;

(2) to prohibit a new information sharing relationship;

(3) to require a new information sharing relationship between any entity and the Federal government, except as specified under section 102(b); or

(4) to modify the authority of a department or agency of the Federal government to protect sources and methods and the national security of the United States.

(b) ANTI-TASKING RESTRICTION.—Nothing in this title shall be construed to permit the Federal government—

(1) to require an entity to share information with the Federal government, except as expressly provided under section 102(b); or

(2) to condition the sharing of cyber threat information with an entity on such entity's provision of cyber threat information to the Federal government.

(c) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this title shall be construed to subject any entity to liability for choosing not to engage in the voluntary activities authorized under this title.

(d) USE AND RETENTION OF INFORMATION.—Nothing in this title shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal government to retain or use any information shared under section 102 for any use other than a use permitted under subsection 102(c)(1).

(e) NO NEW FUNDING.—An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 105. REPORT ON IMPLEMENTATION.

(a) CONTENT OF REPORT.—Not later than 1 year after the date of enactment of this Act, and biennially thereafter, the heads of each department or agency containing a cybersecurity center shall jointly submit, in coordination with the privacy and civil liberties officials of such departments or agencies and the Privacy and Civil Liberties Oversight Board, a detailed report to Congress concerning the implementation of this title, including—

(1) an assessment of the sufficiency of the procedures developed under section 103 of this Act in ensuring that cyber threat information in the possession of the Federal government is provided in an immediate and adequate manner to appropriate entities or, if appropriate, is made publicly available;

(2) an assessment of whether information has been appropriately classified and an accounting of the number of security clearances authorized by the Federal government for purposes of this title;

(3) a review of the type of cyber threat information shared with a cybersecurity center under section 102 of this Act, including whether such information meets the definition of cyber threat information under section 101, the degree to which such information may impact the privacy and civil liberties of individuals, any appropriate metrics to determine any impact of the sharing of such information with the Federal government on privacy and civil liberties, and the adequacy of any steps taken to reduce such impact;

(4) a review of actions taken by the Federal government based on information provided to a cybersecurity center under section 102 of this Act, including the appropriateness of any subsequent use under section 102(c)(1) of this Act and whether there was inappropriate stovepiping within the Federal government of any such information;

(5) a description of any violations of the requirements of this title by the Federal government;

(6) a classified list of entities that received classified information from the Federal government under section 103 of this Act and a description of any indication that such information may not have been appropriately handled;

(7) a summary of any breach of information security, if known, attributable to a specific failure by any entity or the Federal government to act on cyber threat information in the possession of such entity or the Federal government that resulted in substantial economic harm or injury to a specific entity or the Federal government; and

(8) any recommendation for improvements or modifications to the authorities under this title.

(b) FORM OF REPORT.—The report under subsection (a) shall be submitted in unclassified form, but shall include a classified annex.

SEC. 106. INSPECTOR GENERAL REVIEW.

(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency are authorized to review compliance by the cybersecurity centers, and by any Federal department or agency receiving cyber threat information from such cybersecurity centers, with the procedures required under section 102 of this Act.

(b) SCOPE OF REVIEW.—The review under subsection (a) shall consider whether the Federal government has handled such cyber threat information in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title.

(c) REPORT TO CONGRESS.—Each review conducted under this section shall be provided to Congress not later than 30 days after the date of completion of the review.

SEC. 107. TECHNICAL AMENDMENTS.

Section 552(b) of title 5, United States Code, is amended—

(1) in paragraph (8), by striking ''or'';

(2) in paragraph (9), by striking ''wells.'' and inserting ''wells; or''; and

(3) by adding at the end the following:

''(10) information shared with or provided to a cybersecurity center under section 102 of title I of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012.''.

SEC. 108. ACCESS TO CLASSIFIED INFORMATION.

(a) AUTHORIZATION REQUIRED.—No person shall be provided with access to classified information (as defined in section 6.1 of Executive Order 13526 (50 U.S.C. 435 note; relating to classified national security information)) relating to cyber security threats or cyber security vulnerabilities under this title without the appropriate security clearances.

(b) SECURITY CLEARANCES.—The appropriate Federal agencies or departments shall, consistent with applicable procedures and requirements, and if otherwise deemed appropriate, assist an individual in timely obtaining an appropriate security clearance where such individual has been determined to be eligible for such clearance and has a need-to-know (as defined in section 6.1 of that Executive Order) classified information to carry out this title.

TITLE II—COORDINATION OF FEDERAL INFORMATION SECURITY POLICY

SEC. 201. COORDINATION OF FEDERAL INFORMATION SECURITY POLICY.

(a) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by striking subchapters II and III and inserting the following:

''SUBCHAPTER II—INFORMATION SECURITY

''§ 3551. Purposes

''The purposes of this subchapter are—

''(1) to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

''(2) to recognize the highly networked nature of the current Federal computing environment and provide effective government-wide management of policies, directives, standards, and guidelines, as well as effective and nimble oversight of and response to information security risks, including coordination of information security efforts throughout the Federal civilian, national security, and law enforcement communities;

''(3) to provide for development and maintenance of controls required to protect agency information and information systems and contribute to the overall improvement of agency information security posture;

''(4) to provide for the development of tools and methods to assess and respond to real-time situational risk for Federal information system operations and assets; and

''(5) to provide a mechanism for improving agency information security programs through continuous monitoring of agency information systems and streamlined reporting requirements rather than overly prescriptive manual reporting.

''§ 3552. Definitions

''In this subchapter:

''(1) ADEQUATE SECURITY.—The term 'adequate security' means security commensurate with the risk and magnitude of the harm resulting from the unauthorized access to or loss, misuse, destruction, or modification of information.

''(2) AGENCY.—The term 'agency' has the meaning given the term in section 3502 of title 44.

''(3) CYBERSECURITY CENTER.—The term 'cybersecurity center' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

''(4) CYBER THREAT INFORMATION.—The term 'cyber threat information' means information that indicates or describes—

''(A) a technical or operation vulnerability or a cyber threat mitigation measure;

''(B) an action or operation to mitigate a cyber threat;

''(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

''(D) a method of defeating a technical control;

''(E) a method of defeating an operational control;

''(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

''(G) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to inadvertently enable the defeat of a technical or operational control;

''(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

''(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

''(J) any combination of subparagraphs (A) through (I).

''(5) DIRECTOR.—The term 'Director' means the Director of the Office of Management and Budget unless otherwise specified.

''(6) ENVIRONMENT OF OPERATION.—The term 'environment of operation' means the information system and environment in which those systems operate, including changing threats, vulnerabilities, technologies, and missions and business practices.

''(7) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

''(8) INCIDENT.—The term 'incident' means an occurrence that—

''(A) actually or imminently jeopardizes the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores, or transmits; or

''(B) constitutes a violation of law or an imminent threat of violation of a law, a security policy, a security procedure, or an acceptable use policy.

''(9) INFORMATION RESOURCES.—The term 'information resources' has the meaning given the term in section 3502 of title 44.

''(10) INFORMATION SECURITY.—The term 'information security' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

''(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

''(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; or

''(C) availability, by ensuring timely and reliable access to and use of information.

''(11) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44.

''(12) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given the term in section 11101 of title 40.

''(13) MALICIOUS RECONNAISSANCE.—The term 'malicious reconnaissance' means a method for actively probing or passively monitoring an information system for the purpose of discerning technical vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

''(14) NATIONAL SECURITY SYSTEM.—

''(A) IN GENERAL.—The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

''(i) the function, operation, or use of which—

''(I) involves intelligence activities;

''(II) involves cryptologic activities related to national security;

''(III) involves command and control of military forces;

''(IV) involves equipment that is an integral part of a weapon or weapons system; or

''(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

''(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

''(B) LIMITATION.—Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

''(15) OPERATIONAL CONTROL.—The term 'operational control' means a security control for an information system that primarily is implemented and executed by people.

''(16) PERSON.—The term 'person' has the meaning given the term in section 3502 of title 44.

''(17) SECRETARY.—The term 'Secretary' means the Secretary of Commerce unless otherwise specified.

''(18) SECURITY CONTROL.—The term 'security control' means the management, operational, and technical controls, including safeguards or countermeasures, prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

''(19) SIGNIFICANT CYBER INCIDENT.—The term 'significant cyber incident' means a cyber incident resulting in, or an attempted cyber incident that, if successful, would have resulted in—

''(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

''(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

''(20) TECHNICAL CONTROL.—The term 'technical control' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

''§ 3553. Federal information security authority and coordination

''(a) IN GENERAL.—The Secretary, in consultation with the Secretary of Homeland Security, shall—

''(1) issue compulsory and binding policies and directives governing agency information security operations, and require implementation of such policies and directives, including—

''(A) policies and directives consistent with the standards and guidelines promulgated under section 11331 of title 40 to identify and provide information security protections prioritized and commensurate with the risk and impact resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by or on behalf of an agency; or

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(B) minimum operational requirements for Federal Government to protect agency information systems and provide common situational awareness across all agency information systems;

''(C) reporting requirements, consistent with relevant law, regarding information security incidents and cyber threat information;

''(D) requirements for agencywide information security programs;

''(E) performance requirements and metrics for the security of agency information systems;

''(F) training requirements to ensure that agencies are able to fully and timely comply with the policies and directives issued by the Secretary under this subchapter;

''(G) training requirements regarding privacy, civil rights, and civil liberties, and information oversight for agency information security personnel;

''(H) requirements for the annual reports to the Secretary under section 3554(d);

''(I) any other information security operations or information security requirements as determined by the Secretary in coordination with relevant agency heads; and

''(J) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

''(2) review the agencywide information security programs under section 3554; and

''(3) designate an individual or an entity at each cybersecurity center, among other responsibilities—

''(A) to receive reports and information about information security incidents, cyber threat information, and deterioration of security control affecting agency information systems; and

''(B) to act on or share the information under subparagraph (A) in accordance with this subchapter.

''(b) CONSIDERATIONS.—When issuing policies and directives under subsection (a), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology under section 11331 of title 40.

''(c) LIMITATION OF AUTHORITY.—The authorities of the Secretary under this section

shall not apply to national security systems. Information security policies, directives, standards and guidelines for national security systems shall be overseen as directed by the President and, in accordance with that direction, carried out under the authority of the heads of agencies that operate or exercise authority over such national security systems.

''(d) STATUTORY CONSTRUCTION.—Nothing in this subchapter shall be construed to alter or amend any law regarding the authority of any head of an agency over such agency.

''§ 3554. Agency responsibilities

''(a) IN GENERAL.—The head of each agency shall—

''(1) be responsible for—

''(A) complying with the policies and directives issued under section 3553;

''(B) providing information security protections commensurate with the risk resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by the agency or by a contractor of an agency or other organization on behalf of an agency; and

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(C) complying with the requirements of this subchapter, including—

''(i) information security standards and guidelines promulgated under section 11331 of title 40;

''(ii) for any national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued as directed by the President; and

''(iii) for any non-national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued under section 3553;

''(D) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

''(E) reporting and sharing, for an agency operating or exercising control of a national security system, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for national security systems issued as directed by the President; and

''(F) reporting and sharing, for those agencies operating or exercising control of non-national security systems, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for non-national security systems as prescribed under section 3553(a), including information to assist the entity designated under section 3555(a) with the ongoing security analysis under section 3555;

''(2) ensure that each senior agency official provides information security for the information and information systems that support the operations and assets under the senior agency official's control, including by—

''(A) assessing the risk and impact that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

''(B) determining the level of information security appropriate to protect such information and information systems in accordance with policies and directives issued under section 3553(a), and standards and guidelines promulgated under section 11331 of title 40 for information security classifications and related requirements;

''(C) implementing policies, procedures, and capabilities to reduce risks to an acceptable level in a cost-effective manner;

''(D) actively monitoring the effective implementation of information security controls and techniques; and

''(E) reporting information about information security incidents, cyber threat information, and deterioration of security controls in a timely and adequate manner to the entity designated under section 3553(a)(3) in accordance with paragraph (1);

''(3) assess and maintain the resiliency of information technology systems critical to agency mission and operations;

''(4) designate the agency Inspector General (or an independent entity selected in consultation with the Director and the Council of Inspectors General on Integrity and Efficiency if the agency does not have an Inspector General) to conduct the annual independent evaluation required under section 3556, and allow the agency Inspector General to contract with an independent entity to perform such evaluation;

''(5) delegate to the Chief Information Officer or equivalent (or to a senior agency official who reports to the Chief Information Officer or equivalent)—

''(A) the authority and primary responsibility to implement an agencywide information security program; and

''(B) the authority to provide information security for the information collected and maintained by the agency (or by a contractor, other agency, or other source on behalf of the agency) and for the information systems that support the operations, assets, and mission of the agency (including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency);

''(6) delegate to the appropriate agency official (who is responsible for a particular agency system or subsystem) the responsibility to ensure and enforce compliance with all requirements of the agency's agencywide information security program in coordination with the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5);

''(7) ensure that an agency has trained personnel who have obtained any necessary security clearances to permit them to assist the agency in complying with this subchapter;

''(8) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5), in coordination with other senior agency officials, reports to the agency head on the effectiveness of the agencywide information security program, including the progress of any remedial actions; and

''(9) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5) has the necessary qualifications to administer the functions described in this subchapter and has information security duties as a primary duty of that official.

''(b) CHIEF INFORMATION OFFICERS.—Each Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under subsection (a)(5) shall—

''(1) establish and maintain an enterprise security operations capability that on a continuous basis—

''(A) detects, reports, contains, mitigates, and responds to information security incidents that impair adequate security of the agency's information or information system in a timely manner and in accordance with the policies and directives under section 3553; and

''(B) reports any information security incident under subparagraph (A) to the entity designated under section 3555;

''(2) develop, maintain, and oversee an agencywide information security program;

''(3) develop, maintain, and oversee information security policies, procedures, and control techniques to address applicable requirements, including requirements under section 3553 of this title and section 11331 of title 40; and

''(4) train and oversee the agency personnel who have significant responsibility for information security with respect to that responsibility.

''(c) AGENCYWIDE INFORMATION SECURITY PROGRAMS.—

''(1) IN GENERAL.—Each agencywide information security program under subsection (b)(2) shall include—

''(A) relevant security risk assessments, including technical assessments and others related to the acquisition process;

''(B) security testing commensurate with risk and impact;

''(C) mitigation of deterioration of security controls commensurate with risk and impact;

''(D) risk-based continuous monitoring and threat assessment of the operational status and security of agency information systems to enable evaluation of the effectiveness of and compliance with information security policies, procedures, and practices, including a relevant and appropriate selection of security controls of information systems identified in the inventory under section 3505(c);

''(E) operation of appropriate technical capabilities in order to detect, mitigate, report, and respond to information security incidents, cyber threat information, and deterioration of security controls in a manner that is consistent with the policies and directives under section 3553, including—

''(i) mitigating risks associated with such information security incidents;

''(ii) notifying and consulting with the entity designated under section 3555; and

''(iii) notifying and consulting with, as appropriate—

''(I) law enforcement and the relevant Office of the Inspector General; and

''(II) any other entity, in accordance with law and as directed by the President;

''(F) a process to ensure that remedial action is taken to address any deficiencies in the information security policies, procedures, and practices of the agency; and

''(G) a plan and procedures to ensure the continuity of operations for information systems that support the operations and assets of the agency.

''(2) RISK MANAGEMENT STRATEGIES.—Each agencywide information security program under subsection (b)(2) shall include the development and maintenance of a risk management strategy for information security. The risk management strategy shall include—

''(A) consideration of information security incidents, cyber threat information, and deterioration of security controls; and

''(B) consideration of the consequences that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency;

''(3) POLICIES AND PROCEDURES.—Each agencywide information security program under subsection (b)(2) shall include policies and procedures that—

''(A) are based on the risk management strategy under paragraph (2);

''(B) reduce information security risks to an acceptable level in a cost-effective manner;

''(C) ensure that cost-effective and adequate information security is addressed as part of the acquisition and ongoing management of each agency information system; and

''(D) ensure compliance with—

''(i) this subchapter; and

''(ii) any other applicable requirements.

''(4) TRAINING REQUIREMENTS.—Each agencywide information security program under subsection (b)(2) shall include information security, privacy, civil rights, civil liberties, and information oversight training that meets any applicable requirements under section 3553. The training shall inform each information security personnel that has access to agency information systems (including contractors and other users of information systems that support the operations and assets of the agency) of—

''(A) the information security risks associated with the information security personnel's activities; and

''(B) the individual's responsibility to comply with the agency policies and procedures that reduce the risks under subparagraph (A).

''(d) ANNUAL REPORT.—Each agency shall submit a report annually to the Secretary of Homeland Security on its agencywide information security program and information systems.

''§ 3555. Multiagency ongoing threat assessment

''(a) IMPLEMENTATION.—The Director of the Office of Management and Budget, in coordination with the Secretary of Homeland Security, shall designate an entity to implement ongoing security analysis concerning agency information systems—

''(1) based on cyber threat information;

''(2) based on agency information system and environment of operation changes, including—

''(A) an ongoing evaluation of the information system security controls; and

''(B) the security state, risk level, and environment of operation of an agency information system, including—

''(i) a change in risk level due to a new cyber threat;

''(ii) a change resulting from a new technology;

''(iii) a change resulting from the agency's mission; and

''(iv) a change resulting from the business practice; and

''(3) using automated processes to the maximum extent possible—

''(A) to increase information system security;

''(B) to reduce paper-based reporting requirements; and

''(C) to maintain timely and actionable knowledge of the state of the information system security.

''(b) STANDARDS.—The National Institute of Standards and Technology may promulgate standards, in coordination with the Secretary of Homeland Security, to assist an agency with its duties under this section.

''(c) COMPLIANCE.—The head of each appropriate department and agency shall be responsible for ensuring compliance and implementing necessary procedures to comply with this section. The head of each appropriate department and agency, in consultation with the Director of the Office of Management and Budget and the Secretary of Homeland Security, shall—

''(1) monitor compliance under this section;

''(2) develop a timeline and implement for the department or agency—

''(A) adoption of any technology, system, or method that facilitates continuous monitoring and threat assessments of an agency information system;

''(B) adoption or updating of any technology, system, or method that prevents, detects, or remediates a significant cyber incident to a Federal information system of the department or agency that has impeded, or is reasonably likely to impede, the performance of a critical mission of the department or agency; and

''(C) adoption of any technology, system, or method that satisfies a requirement under this section.

''(d) LIMITATION OF AUTHORITY.—The authorities of the Director of the Office of Management and Budget and of the Secretary of Homeland Security under this section shall not apply to national security systems.

''(e) REPORT.—Not later than 6 months after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Government Accountability Office shall issue a report evaluating each agency's status toward implementing this section.

''§ 3556. Independent evaluations

''(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency, in consultation with the Director and the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense, shall issue and maintain criteria for the timely, cost-effective, risk-based, and independent evaluation of each agencywide information security program (and practices) to determine the effectiveness of the agencywide information security program (and practices). The criteria shall include measures to assess any conflicts of interest in the performance of the evaluation and whether the agencywide information security program includes appropriate safeguards against disclosure of information where such disclosure may adversely affect information security.

''(b) ANNUAL INDEPENDENT EVALUATIONS.—Each agency shall perform an annual independent evaluation of its agencywide information security program (and practices) in accordance with the criteria under subsection (a).

''(c) DISTRIBUTION OF REPORTS.—Not later than 30 days after receiving an independent evaluation under subsection (b), each agency head shall transmit a copy of the independent evaluation to the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense.

''(d) NATIONAL SECURITY SYSTEMS.—Evaluations involving national security systems shall be conducted as directed by President.

''§ 3557. National security systems.

''The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

''(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system; and

''(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President.''.

(b) SAVINGS PROVISIONS.—

(1) POLICY AND COMPLIANCE GUIDANCE.—Policy and compliance guidance issued by the Director before the date of enactment of this Act under section 3543(a)(1) of title 44, United States Code (as in effect on the day before the date of enactment of this Act), shall continue in effect, according to its terms, until modified, terminated, superseded, or repealed pursuant to section 3553(a)(1) of title 44, United States Code.

(2) STANDARDS AND GUIDELINES.—Standards and guidelines issued by the Secretary of Commerce or by the Director before the date of enactment of this Act under section 11331(a)(1) of title 40, United States Code, (as in effect on the day before the date of enactment of this Act) shall continue in effect, according to their terms, until modified, terminated, superseded, or repealed pursuant to section 11331(a)(1) of title 40, United States Code, as amended by this Act.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) CHAPTER ANALYSIS.—The chapter analysis for chapter 35 of title 44, United States Code, is amended—

(A) by striking the items relating to sections 3531 through 3538;

(B) by striking the items relating to sections 3541 through 3549; and

(C) by inserting the following:

''3551. Purposes.
''3552. Definitions.
''3553. Federal information security authority and coordination.
''3554. Agency responsibilities.
''3555. Multiagency ongoing threat assessment.
''3556. Independent evaluations.
''3557. National security systems.''.

(2) OTHER REFERENCES.—

(A) Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(1)(A)) is amended by striking ''section 3532(3)'' and inserting ''section 3552''.

(B) Section 2222(j)(5) of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(C) Section 2223(c)(3) of title 10, United States Code, is amended, by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(D) Section 2315 of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(E) Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended—

(i) in subsection (a)(2), by striking ''section 3532(b)(2)'' and inserting ''section 3552'';

(ii) in subsection (c)(3), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iii) in subsection (d)(1), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iv) in subsection (d)(8) by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(v) in subsection (d)(8), by striking ''submitted to the Director'' and inserting ''submitted to the Secretary'';

(vi) in subsection (e)(2), by striking ''section 3532(1) of such title'' and inserting ''section 3552 of title 44''; and

(vii) in subsection (e)(5), by striking ''section 3532(b)(2) of such title'' and inserting ''section 3552 of title 44''.

(F) Section 8(d)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7406(d)(1)) is amended by striking ''section 3534(b)'' and inserting ''section 3554(b)(2)''.

SEC. 202. MANAGEMENT OF INFORMATION TECHNOLOGY.

(a) IN GENERAL.—Section 11331 of title 40, United States Code, is amended to read as follows:

"§ 11331. Responsibilities for Federal information systems standards

''(a) STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO PRESCRIBE.—Except as provided under paragraph (2), the Secretary of Commerce shall prescribe standards and guidelines pertaining to Federal information systems—

''(A) in consultation with the Secretary of Homeland Security; and

''(B) on the basis of standards and guidelines developed by the National Institute of Standards and Technology under paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)(2) and (a)(3)).

''(2) NATIONAL SECURITY SYSTEMS.—Standards and guidelines for national security systems shall be developed, prescribed, enforced, and overseen as otherwise authorized by law and as directed by the President.

''(b) MANDATORY STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO MAKE MANDATORY STANDARDS AND GUIDELINES.—The Secretary of Commerce shall make standards and guidelines under subsection (a)(1) compulsory and binding to the extent determined necessary by the Secretary of Commerce to improve the efficiency of operation or security of Federal information systems.

''(2) REQUIRED MANDATORY STANDARDS AND GUIDELINES.—

''(A) IN GENERAL.—Standards and guidelines under subsection (a)(1) shall include information security standards that—

''(i) provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)); and

''(ii) are otherwise necessary to improve the security of Federal information and information systems.

''(B) BINDING EFFECT.—Information security standards under subparagraph (A) shall be compulsory and binding.

''(c) EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary of Commerce shall exercise the authority conferred by this section subject to direction by the President and in coordination with the Director.

''(d) APPLICATION OF MORE STRINGENT STANDARDS AND GUIDELINES.—The head of an executive agency may employ standards for the cost-effective information security for information systems within or under the supervision of that agency that are more stringent than the standards and guidelines the Secretary of Commerce prescribes under this section if the more stringent standards and guidelines—

''(1) contain at least the applicable standards and guidelines made compulsory and binding by the Secretary of Commerce; and

''(2) are otherwise consistent with the policies, directives, and implementation memoranda issued under section 3553(a) of title 44.

''(e) DECISIONS ON PROMULGATION OF STANDARDS AND GUIDELINES.—The decision by the Secretary of Commerce regarding the promulgation of any standard or guideline under this section shall occur not later than 6 months after the date of submission of the proposed standard to the Secretary of Commerce by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

''(f) NOTICE AND COMMENT.—A decision by the Secretary of Commerce to significantly modify, or not promulgate, a proposed standard submitted to the Secretary by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) shall be made after the public is given an opportunity to comment on the Secretary's proposed decision.

''(g) DEFINITIONS.—In this section:

''(1) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' has the meaning given the term in section 3552 of title 44.

''(2) INFORMATION SECURITY.—The term 'information security' has the meaning given the term in section 3552 of title 44.

''(3) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given the term in section 3552 of title 44.''.

SEC. 203. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 204. TECHNICAL AND CONFORMING AMENDMENTS.

Section 21(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4(b)) is amended—

(1) in paragraph (2), by striking ''and the Director of the Office of Management and Budget'' and inserting '', the Secretary of Commerce, and the Secretary of Homeland Security''; and

(2) in paragraph (3), by inserting '', the Secretary of Homeland Security,'' after ''the Secretary of Commerce''.

SEC. 205. CLARIFICATION OF AUTHORITIES.

Nothing in this title shall be construed to convey any new regulatory authority to any government entity implementing or complying with any provision of this title.

TITLE III—CRIMINAL PENALTIES

SEC. 301. PENALTIES FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030(c) of title 18, United States Code, is amended to read as follows:

''(c) The punishment for an offense under subsection (a) or (b) of this section is—

''(1) a fine under this title or imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(1) of this section;

''(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than 3 years, or both, in the case of an offense under subsection (a)(2); or

''(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2) of this section, if—

''(i) the offense was committed for purposes of commercial advantage or private financial gain;

''(ii) the offense was committed in the furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States, or of any State; or

''(iii) the value of the information obtained, or that would have been obtained if the offense was completed, exceeds $5,000;

''(3) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(3) of this section;

''(4) a fine under this title or imprisonment of not more than 20 years, or both, in the case of an offense under subsection (a)(4) of this section;

''(5)(A) except as provided in subparagraph (C), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A) of this section, if the offense caused—

''(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

''(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

''(iii) physical injury to any person;

''(iv) a threat to public health or safety;

''(v) damage affecting a computer used by, or on behalf of, an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

''(vi) damage affecting 10 or more protected computers during any 1-year period;

''(B) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(B), if the offense caused a harm provided in clause (i) through (vi) of subparagraph (A) of this subsection;

''(C) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both;

''(D) a fine under this title, imprisonment for not more than 10 years, or both, for any other offense under subsection (a)(5);

''(E) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(6) of this section; or

''(F) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(7) of this section.''.

SEC. 302. TRAFFICKING IN PASSWORDS.

Section 1030(a)(6) of title 18, United States Code, is amended to read as follows:

''(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information or means of access through which a protected computer (as defined in subparagraphs (A) and (B) of subsection (e)(2)) may be accessed without authorization.''.

SEC. 303. CONSPIRACY AND ATTEMPTED COMPUTER FRAUD OFFENSES.

Section 1030(b) of title 18, United States Code, is amended by inserting ''as if for the completed offense'' after ''punished as provided''.

SEC. 304. CRIMINAL AND CIVIL FORFEITURE FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030 of title 18, United States Code, is amended by striking subsections (i) and (j) and inserting the following:

''(i) CRIMINAL FORFEITURE.—

''(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

''(A) such persons interest in any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of such violation; and

''(B) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of such violation.

''(2) The criminal forfeiture of property under this subsection, including any seizure and disposition of the property, and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

''(j) CIVIL FORFEITURE.—

''(1) The following shall be subject to forfeiture to the United States and no property right, real or personal, shall exist in them:

''(A) Any property, real or personal, that was used, or intended to be used, to commit

or facilitate the commission of any violation of this section, or a conspiracy to violate this section.

''(B) Any property, real or personal, constituting or derived from any gross proceeds obtained directly or indirectly, or any property traceable to such property, as a result of the commission of any violation of this section, or a conspiracy to violate this section.

''(2) Seizures and forfeitures under this subsection shall be governed by the provisions in chapter 46 relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents and other persons as may be designated for that purpose by the Secretary of Homeland Security or the Attorney General.''.

SEC. 305. DAMAGE TO CRITICAL INFRASTRUCTURE COMPUTERS.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

''§ 1030A. Aggravated damage to a critical infrastructure computer

''(a) DEFINITIONS.—In this section—

''(1) the term 'computer' has the meaning given the term in section 1030;

''(2) the term 'critical infrastructure computer' means a computer that manages or controls systems or assets vital to national defense, national security, national economic security, public health or safety, or any combination of those matters, whether publicly or privately owned or operated, including—

''(A) oil and gas production, storage, conversion, and delivery systems;

''(B) water supply systems;

''(C) telecommunication networks;

''(D) electrical power generation and delivery systems;

''(E) finance and banking systems;

''(F) emergency services;

''(G) transportation systems and services; and

''(H) government operations that provide essential services to the public; and

''(3) the term 'damage' has the meaning given the term in section 1030.

''(b) OFFENSE.—It shall be unlawful, during and in relation to a felony violation of section 1030, to knowingly cause or attempt to cause damage to a critical infrastructure computer if the damage results in (or, in the case of an attempt, if completed, would have resulted in) the substantial impairment—

''(1) of the operation of the critical infrastructure computer; or

''(2) of the critical infrastructure associated with the computer.

''(c) PENALTY.—Any person who violates subsection (b) shall be—

''(1) fined under this title;

''(2) imprisoned for not less than 3 years but not more than 20 years; or

''(3) penalized under paragraphs (1) and (2).

''(d) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

''(1) a court shall not place on probation any person convicted of a violation of this section;

''(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment, including any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for a felony violation of section 1030;

''(3) in determining any term of imprisonment to be imposed for a felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The chapter analysis for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

''1030A. Aggravated damage to a critical infrastructure computer.''.

SEC. 306. LIMITATION ON ACTIONS INVOLVING UNAUTHORIZED USE.

Section 1030(e)(6) of title 18, United States Code, is amended by striking ''alter;'' and inserting ''alter, but does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized;''.

SEC. 307. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

TITLE IV—CYBERSECURITY RESEARCH AND DEVELOPMENT

SEC. 401. NATIONAL HIGH-PERFORMANCE COMPUTING PROGRAM PLANNING AND COORDINATION.

(a) GOALS AND PRIORITIES.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(d) GOALS AND PRIORITIES.—The goals and priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include—

''(1) encouraging and supporting mechanisms for interdisciplinary research and development in networking and information technology, including—

''(A) through collaborations across agencies;

''(B) through collaborations across Program Component Areas;

''(C) through collaborations with industry;

''(D) through collaborations with institutions of higher education;

''(E) through collaborations with Federal laboratories (as defined in section 4 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3703)); and

''(F) through collaborations with international organizations;

''(2) addressing national, multi-agency, multi-faceted challenges of national importance; and

''(3) fostering the transfer of research and development results into new technologies and applications for the benefit of society.''.

(b) DEVELOPMENT OF STRATEGIC PLAN.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(e) STRATEGIC PLAN.—

''(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the agencies under subsection (a)(3)(B), working through the National Science and Technology Council and with the assistance of the Office of Science and Technology Policy shall develop a 5-year strategic plan to guide the activities under subsection (a)(1).

''(2) CONTENTS.—The strategic plan shall specify—

''(A) the near-term objectives for the Program;

''(B) the long-term objectives for the Program;

''(C) the anticipated time frame for achieving the near-term objectives;

''(D) the metrics that will be used to assess any progress made toward achieving the near-term objectives and the long-term objectives; and

''(E) how the Program will achieve the goals and priorities under subsection (d).

''(3) IMPLEMENTATION ROADMAP.—

''(A) IN GENERAL.—The agencies under subsection (a)(3)(B) shall develop and annually update an implementation roadmap for the strategic plan.

''(B) REQUIREMENTS.—The information in the implementation roadmap shall be coordinated with the database under section 102(c) and the annual report under section 101(a)(3). The implementation roadmap shall—

''(i) specify the role of each Federal agency in carrying out or sponsoring research and development to meet the research objectives of the strategic plan, including a description of how progress toward the research objectives will be evaluated, with consideration of any relevant recommendations of the advisory committee;

''(ii) specify the funding allocated to each major research objective of the strategic plan and the source of funding by agency for the current fiscal year; and

''(iii) estimate the funding required for each major research objective of the strategic plan for the next 3 fiscal years.

''(4) RECOMMENDATIONS.—The agencies under subsection (a)(3)(B) shall take into consideration when developing the strategic plan under paragraph (1) the recommendations of—

''(A) the advisory committee under subsection (b); and

''(B) the stakeholders under section 102(a)(3).

''(5) REPORT TO CONGRESS.—The Director of the Office of Science and Technology Policy shall transmit the strategic plan under this subsection, including the implementation roadmap and any updates under paragraph (3), to—

''(A) the advisory committee under subsection (b);

''(B) the Committee on Commerce, Science, and Transportation of the Senate; and

''(C) the Committee on Science and Technology of the House of Representatives.''.

(c) PERIODIC REVIEWS.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(f) PERIODIC REVIEWS.—The agencies under subsection (a)(3)(B) shall—

''(1) periodically assess the contents and funding levels of the Program Component Areas and restructure the Program when warranted, taking into consideration any relevant recommendations of the advisory committee under subsection (b); and

''(2) ensure that the Program includes national, multi-agency, multi-faceted research and development activities, including activities described in section 104.''.

(d) ADDITIONAL RESPONSIBILITIES OF DIRECTOR.—Section 101(a)(2) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(2)) is amended—

(1) by redesignating subparagraphs (E) and (F) as subparagraphs (G) and (H), respectively; and

(2) by inserting after subparagraph (D) the following:

''(E) encourage and monitor the efforts of the agencies participating in the Program to allocate the level of resources and management attention necessary—

''(i) to ensure that the strategic plan under subsection (e) is developed and executed effectively; and

''(ii) to ensure that the objectives of the Program are met;

''(F) working with the Office of Management and Budget and in coordination with the creation of the database under section 102(c), direct the Office of Science and Technology Policy and the agencies participating in the Program to establish a mechanism (consistent with existing law) to track all ongoing and completed research and development projects and associated funding;''.

(e) ADVISORY COMMITTEE.—Section 101(b) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(b)) is amended—

(1) in paragraph (1)—

(A) by inserting after the first sentence the following: ''The co-chairs of the advisory committee shall meet the qualifications of committee members and may be members of the Presidents Council of Advisors on Science and Technology.''; and

(B) by striking ''high-performance'' in subparagraph (D) and inserting ''high-end''; and

(2) by amending paragraph (2) to read as follows:

''(2) In addition to the duties under paragraph (1), the advisory committee shall conduct periodic evaluations of the funding, management, coordination, implementation, and activities of the Program. The advisory committee shall report its findings and recommendations not less frequently than once every 3 fiscal years to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives. The report shall be submitted in conjunction with the update of the strategic plan.''.

(f) REPORT.—Section 101(a)(3) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(3)) is amended—

(1) in subparagraph (C)—

(A) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(B) by striking ''each Program Component Area'' and inserting ''each Program Component Area and each research area supported in accordance with section 104'';

(2) in subparagraph (D)—

(A) by striking ''each Program Component Area,'' and inserting ''each Program Component Area and each research area supported in accordance with section 104,'';

(B) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(C) by striking ''and'' after the semicolon;

(3) by redesignating subparagraph (E) as subparagraph (G); and

(4) by inserting after subparagraph (D) the following:

''(E) include a description of how the objectives for each Program Component Area, and the objectives for activities that involve multiple Program Component Areas, relate to the objectives of the Program identified in the strategic plan under subsection (e);

''(F) include—

''(i) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the next fiscal year by category of activity;

''(ii) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the current fiscal year by category of activity; and

''(iii) the amount of funding provided for the Office of Science and Technology Policy for the current fiscal year by each agency participating in the Program; and''.

(g) DEFINITIONS.—Section 4 of the High-Performance Computing Act of 1991 (15 U.S.C. 5503) is amended—

(1) by redesignating paragraphs (1) and (2) as paragraphs (2) and (3), respectively;

(2) by redesignating paragraph (3) as paragraph (6);

(3) by redesignating paragraphs (6) and (7) as paragraphs (7) and (8), respectively;

(4) by inserting before paragraph (2), as redesignated, the following:

''(1) 'cyber-physical systems' means physical or engineered systems whose networking and information technology functions and physical elements are deeply integrated and are actively connected to the physical world through sensors, actuators, or other means to perform monitoring and control functions;'';

(5) in paragraph (3), as redesignated, by striking ''high-performance computing'' and inserting ''networking and information technology'';

(6) in paragraph (6), as redesignated—

(A) by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(B) by striking ''supercomputer'' and inserting ''high-end computing'';

(7) in paragraph (5), by striking ''network referred to as'' and all that follows through the semicolon and inserting ''network, including advanced computer networks of Federal agencies and departments''; and

(8) in paragraph (7), as redesignated, by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program''.

SEC. 402. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

(a) RESEARCH IN AREAS OF NATIONAL IMPORTANCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.) is amended by adding at the end the following:

''SEC. 104. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

''(a) IN GENERAL.—The Program shall encourage agencies under section 101(a)(3)(B) to support, maintain, and improve national, multi-agency, multi-faceted, research and development activities in networking and information technology directed toward application areas that have the potential for significant contributions to national economic competitiveness and for other significant societal benefits.

''(b) TECHNICAL SOLUTIONS.—An activity under subsection (a) shall be designed to advance the development of research discoveries by demonstrating technical solutions to important problems in areas including—

''(1) cybersecurity;

''(2) health care;

''(3) energy management and low-power systems and devices;

''(4) transportation, including surface and air transportation;

''(5) cyber-physical systems;

''(6) large-scale data analysis and modeling of physical phenomena;

''(7) large scale data analysis and modeling of behavioral phenomena;

''(8) supply chain quality and security; and

''(9) privacy protection and protected disclosure of confidential data.

''(c) RECOMMENDATIONS.—The advisory committee under section 101(b) shall make recommendations to the Program for candidate research and development areas for support under this section.

''(d) CHARACTERISTICS.—

''(1) IN GENERAL.—Research and development activities under this section—

''(A) shall include projects selected on the basis of applications for support through a competitive, merit-based process;

''(B) shall leverage, when possible, Federal investments through collaboration with related State initiatives;

''(C) shall include a plan for fostering the transfer of research discoveries and the results of technology demonstration activities, including from institutions of higher education and Federal laboratories, to industry for commercial development;

''(D) shall involve collaborations among researchers in institutions of higher education and industry; and

''(E) may involve collaborations among nonprofit research institutions and Federal laboratories, as appropriate.

''(2) COST-SHARING.—In selecting applications for support, the agencies under section 101(a)(3)(B) shall give special consideration to projects that include cost sharing from non-Federal sources.

''(3) MULTIDISCIPLINARY RESEARCH CENTERS.—Research and development activities under this section shall be supported through multidisciplinary research centers, including Federal laboratories, that are organized to investigate basic research questions and carry out technology demonstration activities in areas described in subsection (a). Research may be carried out through existing multidisciplinary centers, including those authorized under section 7024(b)(2) of the America COMPETES Act (42 U.S.C. 1862o–10(2)).''.

(b) CYBER-PHYSICAL SYSTEMS.—Section 101(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following:

''(J) provide for increased understanding of the scientific principles of cyber-physical systems and improve the methods available for the design, development, and operation of cyber-physical systems that are characterized by high reliability, safety, and security; and

''(K) provide for research and development on human-computer interactions, visualization, and big data.''.

(c) TASK FORCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.), as amended by section 402(a) of this Act, is amended by adding at the end the following:

''SEC. 105. TASK FORCE.

''(a) ESTABLISHMENT.—Not later than 180 days after the date of enactment the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy under section 102 shall convene a task force to explore mechanisms for carrying out collaborative research and development activities for cyber-physical systems (including the related technologies required to enable these systems) through a consortium or other appropriate entity with participants from institutions of higher education, Federal laboratories, and industry.

''(b) FUNCTIONS.—The task force shall—

''(1) develop options for a collaborative model and an organizational structure for such entity under which the joint research and development activities could be planned,

managed, and conducted effectively, including mechanisms for the allocation of resources among the participants in such entity for support of such activities;

''(2) propose a process for developing a research and development agenda for such entity, including guidelines to ensure an appropriate scope of work focused on nationally significant challenges and requiring collaboration and to ensure the development of related scientific and technological milestones;

''(3) define the roles and responsibilities for the participants from institutions of higher education, Federal laboratories, and industry in such entity;

''(4) propose guidelines for assigning intellectual property rights and for transferring research results to the private sector; and

''(5) make recommendations for how such entity could be funded from Federal, State, and non-governmental sources.

''(c) COMPOSITION.—In establishing the task force under subsection (a), the Director of the Office of Science and Technology Policy shall appoint an equal number of individuals from institutions of higher education and from industry with knowledge and expertise in cyber-physical systems, and may appoint not more than 2 individuals from Federal laboratories.

''(d) REPORT.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy shall transmit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives a report describing the findings and recommendations of the task force.

''(e) TERMINATION.—The task force shall terminate upon transmittal of the report required under subsection (d).

''(f) COMPENSATION AND EXPENSES.—Members of the task force shall serve without compensation.''.

SEC. 403. PROGRAM IMPROVEMENTS.

Section 102 of the High-Performance Computing Act of 1991 (15 U.S.C. 5512) is amended to read as follows:

''SEC. 102. PROGRAM IMPROVEMENTS.

''(a) FUNCTIONS.—The Director of the Office of Science and Technology Policy shall continue—

''(1) to provide technical and administrative support to—

''(A) the agencies participating in planning and implementing the Program, including support needed to develop the strategic plan under section 101(e); and

''(B) the advisory committee under section 101(b);

''(2) to serve as the primary point of contact on Federal networking and information technology activities for government agencies, academia, industry, professional societies, State computing and networking technology programs, interested citizen groups, and others to exchange technical and programmatic information;

''(3) to solicit input and recommendations from a wide range of stakeholders during the development of each strategic plan under section 101(e) by convening at least 1 workshop with invitees from academia, industry, Federal laboratories, and other relevant organizations and institutions;

''(4) to conduct public outreach, including the dissemination of the advisory committee's findings and recommendations, as appropriate;

''(5) to promote access to and early application of the technologies, innovations, and expertise derived from Program activities to agency missions and systems across the Federal Government and to United States industry;

''(6) to ensure accurate and detailed budget reporting of networking and information technology research and development investment; and

''(7) to encourage agencies participating in the Program to use existing programs and resources to strengthen networking and information technology education and training, and increase participation in such fields, including by women and underrepresented minorities.

''(b) SOURCE OF FUNDING.—

''(1) IN GENERAL.—The functions under this section shall be supported by funds from each agency participating in the Program.

''(2) SPECIFICATIONS.—The portion of the total budget of the Office of Science and Technology Policy that is provided by each agency participating in the Program for each fiscal year shall be in the same proportion as each agency's share of the total budget for the Program for the previous fiscal year, as specified in the database under section 102(c).

''(c) DATABASE.—

''(1) IN GENERAL.—The Director of the Office of Science and Technology Policy shall develop and maintain a database of projects funded by each agency for the fiscal year for each Program Component Area.

''(2) PUBLIC ACCESSIBILITY.—The Director of the Office of Science and Technology Policy shall make the database accessible to the public.

''(3) DATABASE CONTENTS.—The database shall include, for each project in the database—

''(A) a description of the project;

''(B) each agency, industry, institution of higher education, Federal laboratory, or international institution involved in the project;

''(C) the source funding of the project (set forth by agency);

''(D) the funding history of the project; and

''(E) whether the project has been completed.''.

SEC. 404. IMPROVING EDUCATION OF NETWORKING AND INFORMATION TECHNOLOGY, INCLUDING HIGH PERFORMANCE COMPUTING.

Section 201(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)) is amended—

(1) by redesignating paragraphs (2) through (4) as paragraphs (3) through (5), respectively; and

(2) by inserting after paragraph (1) the following:

''(2) the National Science Foundation shall use its existing programs, in collaboration with other agencies, as appropriate, to improve the teaching and learning of networking and information technology at all levels of education and to increase participation in networking and information technology fields;''.

SEC. 405. CONFORMING AND TECHNICAL AMENDMENTS TO THE HIGH-PERFORMANCE COMPUTING ACT OF 1991.

(a) SECTION 3.—Section 3 of the High-Performance Computing Act of 1991 (15 U.S.C. 5502) is amended—

(1) in the matter preceding paragraph (1), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(2) in paragraph (1)—

(A) in the matter preceding subparagraph (A), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(B) in subparagraphs (A), (F), and (G), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(C) in subparagraph (H), by striking ''high-performance'' and inserting ''high-end''; and

(3) in paragraph (2)—

(A) by striking ''high-performance computing and'' and inserting ''networking and information technology, and''; and

(B) by striking ''high-performance computing network'' and inserting ''networking and information technology''.

(b) TITLE HEADING.—The heading of title I of the High-Performance Computing Act of 1991 (105 Stat. 1595) is amended by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''.

(c) SECTION 101.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT**'';

(2) in subsection (a)—

(A) in the subsection heading, by striking ''NATIONAL HIGH-PERFORMANCE COMPUTING'' and inserting ''NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT'';

(B) in paragraph (1)—

(i) by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program'';

(ii) in subparagraph (A), by striking ''high-performance computing, including networking'' and inserting ''networking and information technology'';

(iii) in subparagraphs (B) and (G), by striking ''high-performance'' each place it appears and inserting ''high-end''; and

(iv) in subparagraph (C), by striking ''high-performance computing and networking'' and inserting ''high-end computing, distributed, and networking''; and

(C) in paragraph (2)—

(i) in subparagraphs (A) and (C)—

(I) by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(II) by striking ''development, networking,'' each place it appears and inserting ''development,''; and

(ii) in subparagraphs (G) and (H), as redesignated by section 401(d) of this Act, by striking ''high-performance'' each place it appears and inserting ''high-end'';

(3) in subsection (b)(1), in the matter preceding subparagraph (A), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(4) in subsection (c)(1)(A), by striking ''high-performance computing'' and inserting ''networking and information technology''.

(d) SECTION 201.—Section 201(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)(1)) is amended by striking ''high-performance computing and advanced high-speed computer networking'' and inserting ''networking and information technology research and development''.

(e) SECTION 202.—Section 202(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5522(a)) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(f) SECTION 203.—Section 203(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5523(a)) is amended—

(1) in paragraph (1), by striking ''high-performance computing and networking'' and inserting ''networking and information technology''; and

(2) in paragraph (2)(A), by striking ''high-performance'' and inserting ''high-end''.

(g) SECTION 204.—Section 204 of the High-Performance Computing Act of 1991 (15 U.S.C. 5524) is amended—

(1) in subsection (a)(1)—

(A) in subparagraph (A), by striking ''high-performance computing systems and networks'' and inserting ''networking and information technology systems and capabilities'';

(B) in subparagraph (B), by striking ''interoperability of high-performance computing systems in networks and for common user interfaces to systems'' and inserting ''interoperability and usability of networking and information technology systems''; and

(C) in subparagraph (C), by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(2) in subsection (b)—

(A) by striking ''HIGH-PERFORMANCE COMPUTING AND NETWORK'' in the heading and inserting ''NETWORKING AND INFORMATION TECHNOLOGY''; and

(B) by striking ''sensitive''.

(h) SECTION 205.—Section 205(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5525(a)) is amended by striking ''computational'' and inserting ''networking and information technology''.

(i) SECTION 206.—Section 206(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5526(a)) is amended by striking ''computational research'' and inserting ''networking and information technology research''.

(j) SECTION 207.—Section 207 of the High-Performance Computing Act of 1991 (15 U.S.C. 5527) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(k) SECTION 208.—Section 208 of the High-Performance Computing Act of 1991 (15 U.S.C. 5528) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''; and

(2) in subsection (a)—

(A) in paragraph (1), by striking ''High-performance computing and associated'' and inserting ''Networking and information'';

(B) in paragraph (2), by striking ''high-performance computing'' and inserting ''networking and information technologies'';

(C) in paragraph (3), by striking ''high-performance'' and inserting ''high-end'';

(D) in paragraph (4), by striking ''high-performance computers and associated'' and inserting ''networking and information''; and

(E) in paragraph (5), by striking ''high-performance computing and associated'' and inserting ''networking and information''.

SEC. 406. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation, in coordination with the Secretary of Homeland Security, shall carry out a Federal cyber scholarship-for-service program to recruit and train the next generation of information technology professionals and security managers to meet the needs of the cybersecurity mission for the Federal government.

(b) PROGRAM DESCRIPTION AND COMPONENTS.—The program shall—

(1) annually assess the workforce needs of the Federal government for cybersecurity professionals, including network engineers, software engineers, and other experts in order to determine how many scholarships should be awarded annually to ensure that the workforce needs following graduation match the number of scholarships awarded;

(2) provide scholarships for up to 1,000 students per year in their pursuit of undergraduate or graduate degrees in the cybersecurity field, in an amount that may include coverage for full tuition, fees, and a stipend;

(3) require each scholarship recipient, as a condition of receiving a scholarship under the program, to serve in a Federal information technology workforce for a period equal to one and one-half times each year, or partial year, of scholarship received, in addition to an internship in the cybersecurity field, if applicable, following graduation;

(4) provide a procedure for the National Science Foundation or a Federal agency, consistent with regulations of the Office of Personnel Management, to request and fund a security clearance for a scholarship recipient, including providing for clearance during a summer internship and upon graduation; and

(5) provide opportunities for students to receive temporary appointments for meaningful employment in the Federal information technology workforce during school vacation periods and for internships.

(c) HIRING AUTHORITY.—

(1) IN GENERAL.—For purposes of any law or regulation governing the appointment of an individual in the Federal civil service, upon the successful completion of the student's studies, a student receiving a scholarship under the program may—

(A) be hired under section 213.3102(r) of title 5, Code of Federal Regulations; and

(B) be exempt from competitive service.

(2) COMPETITIVE SERVICE.—Upon satisfactory fulfillment of the service term under paragraph (1), an individual may be converted to a competitive service position without competition if the individual meets the requirements for that position.

(d) ELIGIBILITY.—The eligibility requirements for a scholarship under this section shall include that a scholarship applicant—

(1) be a citizen of the United States;

(2) be eligible to be granted a security clearance;

(3) maintain a grade point average of 3.2 or above on a 4.0 scale for undergraduate study or a 3.5 or above on a 4.0 scale for post-graduate study;

(4) demonstrate a commitment to a career in improving the security of the information infrastructure; and

(5) has demonstrated a level of proficiency in math or computer sciences.

(e) FAILURE TO COMPLETE SERVICE OBLIGATION.—

(1) IN GENERAL.—A scholarship recipient under this section shall be liable to the United States under paragraph (2) if the scholarship recipient—

(A) fails to maintain an acceptable level of academic standing in the educational institution in which the individual is enrolled, as determined by the Director;

(B) is dismissed from such educational institution for disciplinary reasons;

(C) withdraws from the program for which the award was made before the completion of such program;

(D) declares that the individual does not intend to fulfill the service obligation under this section;

(E) fails to fulfill the service obligation of the individual under this section; or

(F) loses a security clearance or becomes ineligible for a security clearance.

(2) REPAYMENT AMOUNTS.—

(A) LESS THAN 1 YEAR OF SERVICE.—If a circumstance under paragraph (1) occurs before the completion of 1 year of a service obligation under this section, the total amount of awards received by the individual under this section shall be repaid.

(B) ONE OR MORE YEARS OF SERVICE.—If a circumstance described in subparagraph (D) or (E) of paragraph (1) occurs after the completion of 1 year of a service obligation under this section, the total amount of scholarship awards received by the individual under this section, reduced by the ratio of the number of years of service completed divided by the number of years of service required, shall be repaid.

(f) EVALUATION AND REPORT.—The Director of the National Science Foundation shall—

(1) evaluate the success of recruiting individuals for scholarships under this section and of hiring and retaining those individuals in the public sector workforce, including the annual cost and an assessment of how the program actually improves the Federal workforce; and

(2) periodically report the findings under paragraph (1) to Congress.

(g) AUTHORIZATION OF APPROPRIATIONS.—From amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), the Secretary may use funds to carry out the requirements of this section for fiscal years 2012 through 2013.

SEC. 407. STUDY AND ANALYSIS OF CERTIFICATION AND TRAINING OF INFORMATION INFRASTRUCTURE PROFESSIONALS.

(a) STUDY.—The President shall enter into an agreement with the National Academies to conduct a comprehensive study of government, academic, and private-sector accreditation, training, and certification programs for personnel working in information infrastructure. The agreement shall require the National Academies to consult with sector coordinating councils and relevant governmental agencies, regulatory entities, and nongovernmental organizations in the course of the study.

(b) SCOPE.—The study shall include—

(1) an evaluation of the body of knowledge and various skills that specific categories of personnel working in information infrastructure should possess in order to secure information systems;

(2) an assessment of whether existing government, academic, and private-sector accreditation, training, and certification programs provide the body of knowledge and various skills described in paragraph (1);

(3) an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity talent, including barriers relating to compensation, the hiring process, job classification, and hiring flexibility; and

(4) an analysis of the sources and availability of cybersecurity talent, a comparison of the skills and expertise sought by the Federal Government and the private sector, an examination of the current and future capacity of United States institutions of higher education, including community colleges, to provide current and future cybersecurity professionals, through education and training activities, with those skills sought by the Federal Government, State and local entities, and the private sector.

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the National Academies shall submit to the President and Congress a report on the results of the study. The report shall include—

(1) findings regarding the state of information infrastructure accreditation, training, and certification programs, including specific areas of deficiency and demonstrable progress; and

(2) recommendations for the improvement of information infrastructure accreditation, training, and certification programs.

SEC. 408. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

(a) IN GENERAL.—The Director of the National Institute of Standards and Technology, in coordination with appropriate Federal authorities, shall—

(1) as appropriate, ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to Congress a plan for ensuring such Federal agency coordination.

(b) CONSULTATION WITH THE PRIVATE SECTOR.—In carrying out the activities under subsection (a)(1), the Director shall ensure consultation with appropriate private sector stakeholders.

SEC. 409. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

The Director of the National Institute of Standards and Technology shall continue a program to support the development of technical standards, metrology, testbeds, and conformance criteria, taking into account appropriate user concerns—

(1) to improve interoperability among identity management technologies;

(2) to strengthen authentication methods of identity management systems;

(3) to improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols; and

(4) to improve the usability of identity management systems.

SEC. 410. FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY RESEARCH GRANT AREAS.—Section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking ''property.'' and inserting ''property;''; and

(3) by adding at the end the following:

''(J) secure fundamental protocols that are at the heart of inter-network communications and data exchange;

''(K) system security that addresses the building of secure systems from trusted and untrusted components;

''(L) monitoring and detection; and

''(M) resiliency and rapid recovery methods.''.

(b) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY GRANTS.—Section 4(a)(3) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(3)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Secretary finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(c) COMPUTER AND NETWORK SECURITY CENTERS.—Section 4(b)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7403(b)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Secretary finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(d) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—Section 5(a)(6) of the Cyber Security Research and Development Act (15 U.S.C. 7404(a)(6)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Secretary finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT GRANTS.—Section 5(b)(2) of the Cyber Security Research and Development Act (15 U.S.C. 7404(b)(2)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Secretary finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(f) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY RESEARCH.—Section 5(c)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7404(c)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Secretary finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

SA 2582. Mrs. HUTCHISON (for herself, Mr. MCCAIN, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin) submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 1, strike line 3 and all that follows through page 211, line 6 and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012'' or ''SECURE IT''.

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

TITLE I—FACILITATING SHARING OF CYBER THREAT INFORMATION

SEC. 101. DEFINITIONS.

In this title:

(1) AGENCY.—The term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code.

(2) ANTITRUST LAWS.—The term ''antitrust laws''—

(A) has the meaning given the term in section 1(a) of the Clayton Act (15 U.S.C. 12(a));

(B) includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that section 5 of that Act applies to unfair methods of competition; and

(C) includes any State law that has the same intent and effect as the laws under subparagraphs (A) and (B).

(3) COUNTERMEASURE.—The term ''countermeasure'' means an automated or a manual action with defensive intent to mitigate cyber threats.

(4) CYBER THREAT INFORMATION.—The term ''cyber threat information'' means information that indicates or describes—

(A) a technical or operation vulnerability or a cyber threat mitigation measure;

(B) an action or operation to mitigate a cyber threat;

(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

(D) a method of defeating a technical control;

(E) a method of defeating an operational control;

(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

(G) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to inadvertently enable the defeat of a technical or operational control;

(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to

identify or describe a cybersecurity threat; or

(J) any combination of subparagraphs (A) through (I).

(5) CYBERSECURITY CENTER.—The term ''cybersecurity center'' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

(6) CYBERSECURITY SYSTEM.—The term ''cybersecurity system'' means a system designed or employed to ensure the integrity, confidentiality, or availability of, or to safeguard, a system or network, including measures intended to protect a system or network from—

(A) efforts to degrade, disrupt, or destroy such system or network; or

(B) theft or misappropriations of private or government information, intellectual property, or personally identifiable information.

(7) ENTITY.—

(A) IN GENERAL.—The term ''entity'' means any private entity, non-Federal government agency or department, or State, tribal, or local government agency or department (including an officer, employee, or agent thereof).

(B) INCLUSIONS.—The term ''entity'' includes a government agency or department (including an officer, employee, or agent thereof) of the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States.

(8) FEDERAL INFORMATION SYSTEM.—The term ''Federal information system'' means an information system of a Federal department or agency used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

(9) INFORMATION SECURITY.—The term ''information security'' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; or

(C) availability, by ensuring timely and reliable access to and use of information.

(10) INFORMATION SYSTEM.—The term ''information system'' has the meaning given the term in section 3502 of title 44, United States Code.

(11) LOCAL GOVERNMENT.—The term ''local government'' means any borough, city, county, parish, town, township, village, or other general purpose political subdivision of a State.

(12) MALICIOUS RECONNAISSANCE.—The term ''malicious reconnaissance'' means a method for actively probing or passively monitoring an information system for the purpose of discerning technical vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(13) OPERATIONAL CONTROL.—The term ''operational control'' means a security control for an information system that primarily is implemented and executed by people.

(14) OPERATIONAL VULNERABILITY.—The term ''operational vulnerability'' means any attribute of policy, process, or procedure that could enable or facilitate the defeat of an operational control.

(15) PRIVATE ENTITY.—The term ''private entity'' means any individual or any private group, organization, or corporation, including an officer, employee, or agent thereof.

(16) SIGNIFICANT CYBER INCIDENT.—The term ''significant cyber incident'' means a cyber incident resulting in, or an attempted cyber incident that, if successful, would have resulted in—

(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

(17) TECHNICAL CONTROL.—The term ''technical control'' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

(18) TECHNICAL VULNERABILITY.—The term ''technical vulnerability'' means any attribute of hardware or software that could enable or facilitate the defeat of a technical control.

(19) TRIBAL.—The term ''tribal'' has the meaning given the term ''Indian tribe'' in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

SEC. 102. AUTHORIZATION TO SHARE CYBER THREAT INFORMATION.

(a) VOLUNTARY DISCLOSURE.—

(1) PRIVATE ENTITIES.—Notwithstanding any other provision of law, a private entity may, for the purpose of preventing, investigating, or otherwise mitigating threats to information security, on its own networks, or as authorized by another entity, on such entity's networks, employ countermeasures and use cybersecurity systems in order to obtain, identify, or otherwise possess cyber threat information.

(2) ENTITIES.—Notwithstanding any other provision of law, an entity may disclose cyber threat information to—

(A) a cybersecurity center; or

(B) any other entity in order to assist with preventing, investigating, or otherwise mitigating threats to information security.

(3) INFORMATION SECURITY PROVIDERS.—If the cyber threat information described in paragraph (1) is obtained, identified, or otherwise possessed in the course of providing information security products or services under contract to another entity, that entity shall be given, at any time prior to disclosure of such information, a reasonable opportunity to authorize or prevent such disclosure, to request anonymization of such information, or to request that reasonable efforts be made to safeguard such information that identifies specific persons from unauthorized access or disclosure.

(b) SIGNIFICANT CYBER INCIDENTS INVOLVING FEDERAL INFORMATION SYSTEMS.—

(1) IN GENERAL.—An entity providing electronic communication services, remote computing services, or information security services to a Federal department or agency shall inform the Federal department or agency of a significant cyber incident involving the Federal information system of that Federal department or agency that—

(A) is directly known to the entity as a result of providing such services;

(B) is directly related to the provision of such services by the entity; and

(C) as determined by the entity, has impeded or will impede the performance of a critical mission of the Federal department or agency.

(2) ADVANCE COORDINATION.—A Federal department or agency receiving the services described in paragraph (1) shall coordinate in advance with an entity described in paragraph (1) to develop the parameters of any information that may be provided under paragraph (1), including clarification of the type of significant cyber incident that will impede the performance of a critical mission of the Federal department or agency.

(3) REPORT.—A Federal department or agency shall report information provided under this subsection to a cybersecurity center.

(4) CONSTRUCTION.—Any information provided to a cybersecurity center under paragraph (3) shall be treated in the same manner as information provided to a cybersecurity center under subsection (a).

(c) INFORMATION SHARED WITH OR PROVIDED TO A CYBERSECURITY CENTER.—Cyber threat information provided to a cybersecurity center under this section—

(1) may be disclosed to, retained by, and used by, consistent with otherwise applicable Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal government for a cybersecurity purpose, a national security purpose, or in order to prevent, investigate, or prosecute any of the offenses listed in section 2516 of title 18, United States Code, and such information shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under this paragraph;

(2) may, with the prior written consent of the entity submitting such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(3) shall be considered the commercial, financial, or proprietary information of the entity providing such information to the Federal government and any disclosure outside the Federal government may only be made upon the prior written consent by such entity and shall not constitute a waiver of any applicable privilege or protection provided by law, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(4) shall be deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records;

(5) shall be, without discretion, withheld from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records;

(6) shall not be subject to the rules of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official;

(7) shall not, if subsequently provided to a State, tribal, or local government or government agency, otherwise be disclosed or distributed to any entity by such State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records,

except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent; and

(8) shall not be directly used by any Federal, State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph.

(d) PROCEDURES RELATING TO INFORMATION SHARING WITH A CYBERSECURITY CENTER.—Not later than 60 days after the date of enactment of this Act, the heads of each department or agency containing a cybersecurity center shall jointly develop, promulgate, and submit to Congress procedures to ensure that cyber threat information shared with or provided to—

(1) a cybersecurity center under this section—

(A) may be submitted to a cybersecurity center by an entity, to the greatest extent possible, through a uniform, publicly available process or format that is easily accessible on the website of such cybersecurity center, and that includes the ability to provide relevant details about the cyber threat information and written consent to any subsequent disclosures authorized by this paragraph;

(B) shall immediately be further shared with each cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government;

(C) is handled by the Federal government in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title, and the Federal government may undertake efforts consistent with this subparagraph to limit the impact on privacy and civil liberties of the sharing of cyber threat information with the Federal government; and

(D) except as provided in this section, shall only be used, disclosed, or handled in accordance with the provisions of subsection (c); and

(2) a Federal agency or department under subsection (b) is provided immediately to a cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government.

(e) INFORMATION SHARED BETWEEN ENTITIES.—

(1) IN GENERAL.—An entity sharing cyber threat information with another entity under this title may restrict the use or sharing of such information by such other entity.

(2) FURTHER SHARING.—Cyber threat information shared by any entity with another entity under this title—

(A) shall only be further shared in accordance with any restrictions placed on the sharing of such information by the entity authorizing such sharing, such as appropriate anonymization of such information; and

(B) may not be used by any entity to gain an unfair competitive advantage to the detriment of the entity authorizing the sharing of such information, except that the conduct described in paragraph (3) shall not constitute unfair competitive conduct.

(3) INFORMATION SHARED WITH STATE, TRIBAL, OR LOCAL GOVERNMENT OR GOVERNMENT AGENCY.—Cyber threat information shared with a State, tribal, or local government or government agency under this title—

(A) may, with the prior written consent of the entity sharing such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent;

(B) shall be deemed voluntarily shared information and exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records;

(C) shall not be disclosed or distributed to any entity by the State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent; and

(D) shall not be directly used by any State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this subparagraph.

(4) ANTITRUST EXEMPTION.—The exchange or provision of cyber threat information or assistance between 2 or more private entities under this title shall not be considered a violation of any provision of antitrust laws if exchanged or provided in order to assist with—

(A) facilitating the prevention, investigation, or mitigation of threats to information security; or

(B) communicating or disclosing of cyber threat information to help prevent, investigate or otherwise mitigate the effects of a threat to information security.

(5) NO RIGHT OR BENEFIT.—The provision of cyber threat information to an entity under this section shall not create a right or a benefit to similar information by such entity or any other entity.

(f) FEDERAL PREEMPTION.—

(1) IN GENERAL.—This section supersedes any statute or other law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this section.

(2) STATE LAW ENFORCEMENT.—Nothing in this section shall be construed to supersede any statute or other law of a State or political subdivision of a State concerning the use of authorized law enforcement techniques.

(3) PUBLIC DISCLOSURE.—No information shared with or provided to a State, tribal, or local government or government agency pursuant to this section shall be made publicly available pursuant to any State, tribal, or local law requiring disclosure of information or records.

(g) CIVIL AND CRIMINAL LIABILITY.—

(1) GENERAL PROTECTIONS.—

(A) PRIVATE ENTITIES.—No cause of action shall lie or be maintained in any court against any private entity for—

(i) the use of countermeasures and cybersecurity systems as authorized by this title;

(ii) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(iii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such private entity.

(B) ENTITIES.—No cause of action shall lie or be maintained in any court against any entity for—

(i) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(ii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such entity.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed as creating any immunity against, or otherwise affecting, any action brought by the Federal government, or any agency or department thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, and use of classified information.

(h) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this section shall be construed to limit or prohibit otherwise lawful disclosures of communications, records, or other information by a private entity to any other governmental or private entity not covered under this section.

(i) WHISTLEBLOWER PROTECTION.—Nothing in this Act shall be construed to preempt or preclude any employee from exercising rights currently provided under any whistleblower law, rule, or regulation.

(j) RELATIONSHIP TO OTHER LAWS.—The submission of cyber threat information under this section to a cybersecurity center shall not affect any requirement under any other provision of law for an entity to provide information to the Federal government.

SEC. 103. INFORMATION SHARING BY THE FEDERAL GOVERNMENT.

(a) CLASSIFIED INFORMATION.—

(1) PROCEDURES.—Consistent with the protection of intelligence sources and methods, and as otherwise determined appropriate, the Director of National Intelligence and the Secretary of Defense, in consultation with the heads of the appropriate Federal departments or agencies, shall develop and promulgate procedures to facilitate and promote—

(A) the immediate sharing, through the cybersecurity centers, of classified cyber threat information in the possession of the Federal government with appropriately cleared representatives of any appropriate entity; and

(B) the declassification and immediate sharing, through the cybersecurity centers, with any entity or, if appropriate, public availability of cyber threat information in the possession of the Federal government;

(2) HANDLING OF CLASSIFIED INFORMATION.—The procedures developed under paragraph (1) shall ensure that each entity receiving classified cyber threat information pursuant to this section has acknowledged in writing the ongoing obligation to comply with all laws, executive orders, and procedures concerning the appropriate handling, disclosure, or use of classified information.

(b) UNCLASSIFIED CYBER THREAT INFORMATION.—The heads of each department or agency containing a cybersecurity center shall jointly develop and promulgate procedures that ensure that, consistent with the provisions of this section, unclassified, including controlled unclassified, cyber threat information in the possession of the Federal government—

(1) is shared, through the cybersecurity centers, in an immediate and adequate manner with appropriate entities; and

(2) if appropriate, is made publicly available.

(c) DEVELOPMENT OF PROCEDURES.—

(1) IN GENERAL.—The procedures developed under this section shall incorporate, to the greatest extent possible, existing processes utilized by sector specific information sharing and analysis centers.

(2) COORDINATION WITH ENTITIES.—In developing the procedures required under this section, the Director of National Intelligence and the heads of each department or agency containing a cybersecurity center shall coordinate with appropriate entities to ensure that protocols are implemented that will facilitate and promote the sharing of cyber threat information by the Federal government.

(d) ADDITIONAL RESPONSIBILITIES OF CYBERSECURITY CENTERS.—Consistent with section 102, a cybersecurity center shall—

(1) facilitate information sharing, interaction, and collaboration among and between cybersecurity centers and—

(A) other Federal entities;

(B) any entity; and

(C) international partners, in consultation with the Secretary of State;

(2) disseminate timely and actionable cybersecurity threat, vulnerability, mitigation, and warning information, including alerts, advisories, indicators, signatures, and mitigation and response measures, to improve the security and protection of information systems; and

(3) coordinate with other Federal entities, as appropriate, to integrate information from across the Federal government to provide situational awareness of the cybersecurity posture of the United States.

(e) SHARING WITHIN THE FEDERAL GOVERNMENT.—The heads of appropriate Federal departments and agencies shall ensure that cyber threat information in the possession of such Federal departments or agencies that relates to the prevention, investigation, or mitigation of threats to information security across the Federal government is shared effectively with the cybersecurity centers.

(f) SUBMISSION TO CONGRESS.—Not later than 60 days after the date of enactment of this Act, the Director of National Intelligence, in coordination with the appropriate head of a department or an agency containing a cybersecurity center, shall submit the procedures required by this section to Congress.

SEC. 104. CONSTRUCTION.

(a) INFORMATION SHARING RELATIONSHIPS.—Nothing in this title shall be construed—

(1) to limit or modify an existing information sharing relationship;

(2) to prohibit a new information sharing relationship;

(3) to require a new information sharing relationship between any entity and the Federal government, except as specified under section 102(b); or

(4) to modify the authority of a department or agency of the Federal government to protect sources and methods and the national security of the United States.

(b) ANTI-TASKING RESTRICTION.—Nothing in this title shall be construed to permit the Federal government—

(1) to require an entity to share information with the Federal government, except as expressly provided under section 102(b); or

(2) to condition the sharing of cyber threat information with an entity on such entity's provision of cyber threat information to the Federal government.

(c) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this title shall be construed to subject any entity to liability for choosing not to engage in the voluntary activities authorized under this title.

(d) USE AND RETENTION OF INFORMATION.—Nothing in this title shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal government to retain or use any information shared under section 102 for any use other than a use permitted under subsection 102(c)(1).

(e) NO NEW FUNDING.—An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 105. REPORT ON IMPLEMENTATION.

(a) CONTENT OF REPORT.—Not later than 1 year after the date of enactment of this Act, and biennially thereafter, the heads of each department or agency containing a cybersecurity center shall jointly submit, in coordination with the privacy and civil liberties officials of such departments or agencies and the Privacy and Civil Liberties Oversight Board, a detailed report to Congress concerning the implementation of this title, including—

(1) an assessment of the sufficiency of the procedures developed under section 103 of this Act in ensuring that cyber threat information in the possession of the Federal government is provided in an immediate and adequate manner to appropriate entities or, if appropriate, is made publicly available;

(2) an assessment of whether information has been appropriately classified and an accounting of the number of security clearances authorized by the Federal government for purposes of this title;

(3) a review of the type of cyber threat information shared with a cybersecurity center under section 102 of this Act, including whether such information meets the definition of cyber threat information under section 101, the degree to which such information may impact the privacy and civil liberties of individuals, any appropriate metrics to determine any impact of the sharing of such information with the Federal government on privacy and civil liberties, and the adequacy of any steps taken to reduce such impact;

(4) a review of actions taken by the Federal government based on information provided to a cybersecurity center under section 102 of this Act, including the appropriateness of any subsequent use under section 102(c)(1) of this Act and whether there was inappropriate stovepiping within the Federal government of any such information;

(5) a description of any violations of the requirements of this title by the Federal government;

(6) a classified list of entities that received classified information from the Federal government under section 103 of this Act and a description of any indication that such information may not have been appropriately handled;

(7) a summary of any breach of information security, if known, attributable to a specific failure by any entity or the Federal government to act on cyber threat information in the possession of such entity or the Federal government that resulted in substantial economic harm or injury to a specific entity or the Federal government; and

(8) any recommendation for improvements or modifications to the authorities under this title.

(b) FORM OF REPORT.—The report under subsection (a) shall be submitted in unclassified form, but shall include a classified annex.

SEC. 106. INSPECTOR GENERAL REVIEW.

(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency are authorized to review compliance by the cybersecurity centers, and by any Federal department or agency receiving cyber threat information from such cybersecurity centers, with the procedures required under section 102 of this Act.

(b) SCOPE OF REVIEW.—The review under subsection (a) shall consider whether the Federal government has handled such cyber threat information in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title.

(c) REPORT TO CONGRESS.—Each review conducted under this section shall be provided to Congress not later than 30 days after the date of completion of the review.

SEC. 107. TECHNICAL AMENDMENTS.

Section 552(b) of title 5, United States Code, is amended—

(1) in paragraph (8), by striking ''or'';

(2) in paragraph (9), by striking ''wells.'' and inserting ''wells; or''; and

(3) by adding at the end the following:

''(10) information shared with or provided to a cybersecurity center under section 102 of title I of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012.''.

SEC. 108. ACCESS TO CLASSIFIED INFORMATION.

(a) AUTHORIZATION REQUIRED.—No person shall be provided with access to classified information (as defined in section 6.1 of Executive Order 13526 (50 U.S.C. 435 note; relating to classified national security information)) relating to cyber security threats or cyber security vulnerabilities under this title without the appropriate security clearances.

(b) SECURITY CLEARANCES.—The appropriate Federal agencies or departments shall, consistent with applicable procedures and requirements, and if otherwise deemed appropriate, assist an individual in timely obtaining an appropriate security clearance where such individual has been determined to be eligible for such clearance and has a need-to-know (as defined in section 6.1 of that Executive Order) classified information to carry out this title.

TITLE II—COORDINATION OF FEDERAL INFORMATION SECURITY POLICY

SEC. 201. COORDINATION OF FEDERAL INFORMATION SECURITY POLICY.

(a) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by striking subchapters II and III and inserting the following:

''SUBCHAPTER II—INFORMATION SECURITY

''§ 3551. Purposes

''The purposes of this subchapter are—

''(1) to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

''(2) to recognize the highly networked nature of the current Federal computing environment and provide effective government-wide management of policies, directives, standards, and guidelines, as well as effective and nimble oversight of and response to information security risks, including coordination of information security efforts throughout the Federal civilian, national security, and law enforcement communities;

''(3) to provide for development and maintenance of controls required to protect agency information and information systems and contribute to the overall improvement of agency information security posture;

''(4) to provide for the development of tools and methods to assess and respond to real-time situational risk for Federal information system operations and assets; and

''(5) to provide a mechanism for improving agency information security programs through continuous monitoring of agency information systems and streamlined reporting requirements rather than overly prescriptive manual reporting.

''§ 3552. Definitions

''In this subchapter:

''(1) ADEQUATE SECURITY.—The term 'adequate security' means security commensurate with the risk and magnitude of the

harm resulting from the unauthorized access to or loss, misuse, destruction, or modification of information.

''(2) AGENCY.—The term 'agency' has the meaning given the term in section 3502 of title 44.

''(3) CYBERSECURITY CENTER.—The term 'cybersecurity center' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

''(4) CYBER THREAT INFORMATION.—The term 'cyber threat information' means information that indicates or describes—

''(A) a technical or operation vulnerability or a cyber threat mitigation measure;

''(B) an action or operation to mitigate a cyber threat;

''(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

''(D) a method of defeating a technical control;

''(E) a method of defeating an operational control;

''(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

''(G) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to inadvertently enable the defeat of a technical or operational control;

''(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

''(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

''(J) any combination of subparagraphs (A) through (I).

''(5) DIRECTOR.—The term 'Director' means the Director of the Office of Management and Budget unless otherwise specified.

''(6) ENVIRONMENT OF OPERATION.—The term 'environment of operation' means the information system and environment in which those systems operate, including changing threats, vulnerabilities, technologies, and missions and business practices.

''(7) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

''(8) INCIDENT.—The term 'incident' means an occurrence that—

''(A) actually or imminently jeopardizes the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores, or transmits; or

''(B) constitutes a violation of law or an imminent threat of violation of a law, a security policy, a security procedure, or an acceptable use policy.

''(9) INFORMATION RESOURCES.—The term 'information resources' has the meaning given the term in section 3502 of title 44.

''(10) INFORMATION SECURITY.—The term 'information security' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

''(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

''(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; or

''(C) availability, by ensuring timely and reliable access to and use of information.

''(11) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44.

''(12) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given the term in section 11101 of title 40.

''(13) MALICIOUS RECONNAISSANCE.—The term 'malicious reconnaissance' means a method for actively probing or passively monitoring an information system for the purpose of discerning technical vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

''(14) NATIONAL SECURITY SYSTEM.—

''(A) IN GENERAL.—The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

''(i) the function, operation, or use of which—

''(I) involves intelligence activities;

''(II) involves cryptologic activities related to national security;

''(III) involves command and control of military forces;

''(IV) involves equipment that is an integral part of a weapon or weapons system; or

''(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

''(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

''(B) LIMITATION.—Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

''(15) OPERATIONAL CONTROL.—The term 'operational control' means a security control for an information system that primarily is implemented and executed by people.

''(16) PERSON.—The term 'person' has the meaning given the term in section 3502 of title 44.

''(17) SECRETARY.—The term 'Secretary' means the Secretary of Commerce unless otherwise specified.

''(18) SECURITY CONTROL.—The term 'security control' means the management, operational, and technical controls, including safeguards or countermeasures, prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

''(19) SIGNIFICANT CYBER INCIDENT.—The term 'significant cyber incident' means a cyber incident resulting in, or an attempted cyber incident that, if successful, would have resulted in—

''(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

''(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

''(20) TECHNICAL CONTROL.—The term 'technical control' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

''§ 3553. Federal information security authority and coordination

''(a) IN GENERAL.—The Secretary, in consultation with the Secretary of Homeland Security, shall—

''(1) issue compulsory and binding policies and directives governing agency information security operations, and require implementation of such policies and directives, including—

''(A) policies and directives consistent with the standards and guidelines promulgated under section 11331 of title 40 to identify and provide information security protections prioritized and commensurate with the risk and impact resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by or on behalf of an agency; or

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(B) minimum operational requirements for Federal Government to protect agency information systems and provide common situational awareness across all agency information systems;

''(C) reporting requirements, consistent with relevant law, regarding information security incidents and cyber threat information;

''(D) requirements for agencywide information security programs;

''(E) performance requirements and metrics for the security of agency information systems;

''(F) training requirements to ensure that agencies are able to fully and timely comply with the policies and directives issued by the Secretary under this subchapter;

''(G) training requirements regarding privacy, civil rights, and civil liberties, and information oversight for agency information security personnel;

''(H) requirements for the annual reports to the Secretary under section 3554(d);

''(I) any other information security operations or information security requirements as determined by the Secretary in coordination with relevant agency heads; and

''(J) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

''(2) review the agencywide information security programs under section 3554; and

''(3) designate an individual or an entity at each cybersecurity center, among other responsibilities—

''(A) to receive reports and information about information security incidents, cyber threat information, and deterioration of security control affecting agency information systems; and

''(B) to act on or share the information under subparagraph (A) in accordance with this subchapter.

''(b) CONSIDERATIONS.—When issuing policies and directives under subsection (a), the

Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology under section 11331 of title 40.

''(c) LIMITATION OF AUTHORITY.—The authorities of the Secretary under this section shall not apply to national security systems. Information security policies, directives, standards and guidelines for national security systems shall be overseen as directed by the President and, in accordance with that direction, carried out under the authority of the heads of agencies that operate or exercise authority over such national security systems.

''(d) STATUTORY CONSTRUCTION.—Nothing in this subchapter shall be construed to alter or amend any law regarding the authority of any head of an agency over such agency.

''§ 3554. Agency responsibilities

''(a) IN GENERAL.—The head of each agency shall—

''(1) be responsible for—

''(A) complying with the policies and directives issued under section 3553;

''(B) providing information security protections commensurate with the risk resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by the agency or by a contractor of an agency or other organization on behalf of an agency; and

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(C) complying with the requirements of this subchapter, including—

''(i) information security standards and guidelines promulgated under section 11331 of title 40;

''(ii) for any national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued as directed by the President; and

''(iii) for any non-national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued under section 3553;

''(D) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

''(E) reporting and sharing, for an agency operating or exercising control of a national security system, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for national security systems issued as directed by the President; and

''(F) reporting and sharing, for those agencies operating or exercising control of non-national security systems, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for non-national security systems as prescribed under section 3553(a), including information to assist the entity designated under section 3555(a) with the ongoing security analysis under section 3555;

''(2) ensure that each senior agency official provides information security for the information and information systems that support the operations and assets under the senior agency official's control, including by—

''(A) assessing the risk and impact that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

''(B) determining the level of information security appropriate to protect such information and information systems in accordance with policies and directives issued under section 3553(a), and standards and guidelines promulgated under section 11331 of title 40 for information security classifications and related requirements;

''(C) implementing policies, procedures, and capabilities to reduce risks to an acceptable level in a cost-effective manner;

''(D) actively monitoring the effective implementation of information security controls and techniques; and

''(E) reporting information about information security incidents, cyber threat information, and deterioration of security controls in a timely and adequate manner to the entity designated under section 3553(a)(3) in accordance with paragraph (1);

''(3) assess and maintain the resiliency of information technology systems critical to agency mission and operations;

''(4) designate the agency Inspector General (or an independent entity selected in consultation with the Director and the Council of Inspectors General on Integrity and Efficiency if the agency does not have an Inspector General) to conduct the annual independent evaluation required under section 3556, and allow the agency Inspector General to contract with an independent entity to perform such evaluation;

''(5) delegate to the Chief Information Officer or equivalent (or to a senior agency official who reports to the Chief Information Officer or equivalent)—

''(A) the authority and primary responsibility to implement an agencywide information security program; and

''(B) the authority to provide information security for the information collected and maintained by the agency (or by a contractor, other agency, or other source on behalf of the agency) and for the information systems that support the operations, assets, and mission of the agency (including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency);

''(6) delegate to the appropriate agency official (who is responsible for a particular agency system or subsystem) the responsibility to ensure and enforce compliance with all requirements of the agency's agencywide information security program in coordination with the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5);

''(7) ensure that an agency has trained personnel who have obtained any necessary security clearances to permit them to assist the agency in complying with this subchapter;

''(8) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5), in coordination with other senior agency officials, reports to the agency head on the effectiveness of the agencywide information security program, including the progress of any remedial actions; and

''(9) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5) has the necessary qualifications to administer the functions described in this subchapter and has information security duties as a primary duty of that official.

''(b) CHIEF INFORMATION OFFICERS.—Each Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under subsection (a)(5) shall—

''(1) establish and maintain an enterprise security operations capability that on a continuous basis—

''(A) detects, reports, contains, mitigates, and responds to information security incidents that impair adequate security of the agency's information or information system in a timely manner and in accordance with the policies and directives under section 3553; and

''(B) reports any information security incident under subparagraph (A) to the entity designated under section 3555;

''(2) develop, maintain, and oversee an agencywide information security program;

''(3) develop, maintain, and oversee information security policies, procedures, and control techniques to address applicable requirements, including requirements under section 3553 of this title and section 11331 of title 40; and

''(4) train and oversee the agency personnel who have significant responsibility for information security with respect to that responsibility.

''(c) AGENCYWIDE INFORMATION SECURITY PROGRAMS.—

''(1) IN GENERAL.—Each agencywide information security program under subsection (b)(2) shall include—

''(A) relevant security risk assessments, including technical assessments and others related to the acquisition process;

''(B) security testing commensurate with risk and impact;

''(C) mitigation of deterioration of security controls commensurate with risk and impact;

''(D) risk-based continuous monitoring and threat assessment of the operational status and security of agency information systems to enable evaluation of the effectiveness of and compliance with information security policies, procedures, and practices, including a relevant and appropriate selection of security controls of information systems identified in the inventory under section 3505(c);

''(E) operation of appropriate technical capabilities in order to detect, mitigate, report, and respond to information security incidents, cyber threat information, and deterioration of security controls in a manner that is consistent with the policies and directives under section 3553, including—

''(i) mitigating risks associated with such information security incidents;

''(ii) notifying and consulting with the entity designated under section 3555; and

''(iii) notifying and consulting with, as appropriate—

''(I) law enforcement and the relevant Office of the Inspector General; and

''(II) any other entity, in accordance with law and as directed by the President;

''(F) a process to ensure that remedial action is taken to address any deficiencies in the information security policies, procedures, and practices of the agency; and

''(G) a plan and procedures to ensure the continuity of operations for information systems that support the operations and assets of the agency.

''(2) RISK MANAGEMENT STRATEGIES.—Each agencywide information security program under subsection (b)(2) shall include the development and maintenance of a risk management strategy for information security. The risk management strategy shall include—

''(A) consideration of information security incidents, cyber threat information, and deterioration of security controls; and

''(B) consideration of the consequences that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency;

''(3) POLICIES AND PROCEDURES.—Each agencywide information security program under subsection (b)(2) shall include policies and procedures that—

''(A) are based on the risk management strategy under paragraph (2);

''(B) reduce information security risks to an acceptable level in a cost-effective manner;

''(C) ensure that cost-effective and adequate information security is addressed as part of the acquisition and ongoing management of each agency information system; and

''(D) ensure compliance with—

''(i) this subchapter; and

''(ii) any other applicable requirements.

''(4) TRAINING REQUIREMENTS.—Each agencywide information security program under subsection (b)(2) shall include information security, privacy, civil rights, civil liberties, and information oversight training that meets any applicable requirements under section 3553. The training shall inform each information security personnel that has access to agency information systems (including contractors and other users of information systems that support the operations and assets of the agency) of—

''(A) the information security risks associated with the information security personnel's activities; and

''(B) the individual's responsibility to comply with the agency policies and procedures that reduce the risks under subparagraph (A).

''(d) ANNUAL REPORT.—Each agency shall submit a report annually to the Secretary of Homeland Security on its agencywide information security program and information systems.

''§ 3555. Multiagency ongoing threat assessment

''(a) IMPLEMENTATION.—The Director of the Office of Management and Budget, in coordination with the Secretary of Homeland Security, shall designate an entity to implement ongoing security analysis concerning agency information systems—

''(1) based on cyber threat information;

''(2) based on agency information system and environment of operation changes, including—

''(A) an ongoing evaluation of the information system security controls; and

''(B) the security state, risk level, and environment of operation of an agency information system, including—

''(i) a change in risk level due to a new cyber threat;

''(ii) a change resulting from a new technology;

''(iii) a change resulting from the agency's mission; and

''(iv) a change resulting from the business practice; and

''(3) using automated processes to the maximum extent possible—

''(A) to increase information system security;

''(B) to reduce paper-based reporting requirements; and

''(C) to maintain timely and actionable knowledge of the state of the information system security.

''(b) STANDARDS.—The National Institute of Standards and Technology may promulgate standards, in coordination with the Secretary of Homeland Security, to assist an agency with its duties under this section.

''(c) COMPLIANCE.—The head of each appropriate department and agency shall be responsible for ensuring compliance and implementing necessary procedures to comply with this section. The head of each appropriate department and agency, in consultation with the Director of the Office of Management and Budget and the Secretary of Homeland Security, shall—

''(1) monitor compliance under this section;

''(2) develop a timeline and implement for the department or agency—

''(A) adoption of any technology, system, or method that facilitates continuous monitoring and threat assessments of an agency information system;

''(B) adoption or updating of any technology, system, or method that prevents, detects, or remediates a significant cyber incident to a Federal information system of the department or agency that has impeded, or is reasonably likely to impede, the performance of a critical mission of the department or agency; and

''(C) adoption of any technology, system, or method that satisfies a requirement under this section.

''(d) LIMITATION OF AUTHORITY.—The authorities of the Director of the Office of Management and Budget and of the Secretary of Homeland Security under this section shall not apply to national security systems.

''(e) REPORT.—Not later than 6 months after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Government Accountability Office shall issue a report evaluating each agency's status toward implementing this section.

''§ 3556. Independent evaluations

''(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency, in consultation with the Director and the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense, shall issue and maintain criteria for the timely, cost-effective, risk-based, and independent evaluation of each agencywide information security program (and practices) to determine the effectiveness of the agencywide information security program (and practices). The criteria shall include measures to assess any conflicts of interest in the performance of the evaluation and whether the agencywide information security program includes appropriate safeguards against disclosure of information where such disclosure may adversely affect information security.

''(b) ANNUAL INDEPENDENT EVALUATIONS.—Each agency shall perform an annual independent evaluation of its agencywide information security program (and practices) in accordance with the criteria under subsection (a).

''(c) DISTRIBUTION OF REPORTS.—Not later than 30 days after receiving an independent evaluation under subsection (b), each agency head shall transmit a copy of the independent evaluation to the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense.

''(d) NATIONAL SECURITY SYSTEMS.—Evaluations involving national security systems shall be conducted as directed by President.

''§ 3557. National security systems.

''The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

''(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system; and

''(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President.''.

(b) SAVINGS PROVISIONS.—

(1) POLICY AND COMPLIANCE GUIDANCE.—Policy and compliance guidance issued by the Director before the date of enactment of this Act under section 3543(a)(1) of title 44, United States Code (as in effect on the day before the date of enactment of this Act), shall continue in effect, according to its terms, until modified, terminated, superseded, or repealed pursuant to section 3553(a)(1) of title 44, United States Code.

(2) STANDARDS AND GUIDELINES.—Standards and guidelines issued by the Secretary of Commerce or by the Director before the date of enactment of this Act under section 11331(a)(1) of title 40, United States Code, (as in effect on the day before the date of enactment of this Act) shall continue in effect, according to their terms, until modified, terminated, superseded, or repealed pursuant to section 11331(a)(1) of title 40, United States Code, as amended by this Act.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) CHAPTER ANALYSIS.—The chapter analysis for chapter 35 of title 44, United States Code, is amended—

(A) by striking the items relating to sections 3531 through 3538;

(B) by striking the items relating to sections 3541 through 3549; and

(C) by inserting the following:

''3551. Purposes.
''3552. Definitions.
''3553. Federal information security authority and coordination.
''3554. Agency responsibilities.
''3555. Multiagency ongoing threat assessment.
''3556. Independent evaluations.
''3557. National security systems.''.

(2) OTHER REFERENCES.—

(A) Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(1)(A)) is amended by striking ''section 3532(3)'' and inserting ''section 3552''.

(B) Section 2222(j)(5) of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(C) Section 2223(c)(3) of title 10, United States Code, is amended, by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(D) Section 2315 of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(E) Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended—

(i) in subsection (a)(2), by striking ''section 3532(b)(2)'' and inserting ''section 3552'';

(ii) in subsection (c)(3), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iii) in subsection (d)(1), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iv) in subsection (d)(8) by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(v) in subsection (d)(8), by striking ''submitted to the Director'' and inserting ''submitted to the Secretary'';

(vi) in subsection (e)(2), by striking ''section 3532(1) of such title'' and inserting ''section 3552 of title 44''; and

(vii) in subsection (e)(5), by striking ''section 3532(b)(2) of such title'' and inserting ''section 3552 of title 44''.

(F) Section 8(d)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7406(d)(1)) is amended by striking ''section 3534(b)'' and inserting ''section 3554(b)(2)''.

SEC. 202. MANAGEMENT OF INFORMATION TECHNOLOGY.

(a) IN GENERAL.—Section 11331 of title 40, United States Code, is amended to read as follows:

''§ 11331. Responsibilities for Federal information systems standards

''(a) STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO PRESCRIBE.—Except as provided under paragraph (2), the Secretary of Commerce shall prescribe standards and guidelines pertaining to Federal information systems—

''(A) in consultation with the Secretary of Homeland Security; and

''(B) on the basis of standards and guidelines developed by the National Institute of Standards and Technology under paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)(2) and (a)(3)).

''(2) NATIONAL SECURITY SYSTEMS.—Standards and guidelines for national security systems shall be developed, prescribed, enforced, and overseen as otherwise authorized by law and as directed by the President.

''(b) MANDATORY STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO MAKE MANDATORY STANDARDS AND GUIDELINES.—The Secretary of Commerce shall make standards and guidelines under subsection (a)(1) compulsory and binding to the extent determined necessary by the Secretary of Commerce to improve the efficiency of operation or security of Federal information systems.

''(2) REQUIRED MANDATORY STANDARDS AND GUIDELINES.—

''(A) IN GENERAL.—Standards and guidelines under subsection (a)(1) shall include information security standards that—

''(i) provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)); and

''(ii) are otherwise necessary to improve the security of Federal information and information systems.

''(B) BINDING EFFECT.—Information security standards under subparagraph (A) shall be compulsory and binding.

''(c) EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary of Commerce shall exercise the authority conferred by this section subject to direction by the President and in coordination with the Director.

''(d) APPLICATION OF MORE STRINGENT STANDARDS AND GUIDELINES.—The head of an executive agency may employ standards for the cost-effective information security for information systems within or under the supervision of that agency that are more stringent than the standards and guidelines the Secretary of Commerce prescribes under this section if the more stringent standards and guidelines—

''(1) contain at least the applicable standards and guidelines made compulsory and binding by the Secretary of Commerce; and

''(2) are otherwise consistent with the policies, directives, and implementation memoranda issued under section 3553(a) of title 44.

''(e) DECISIONS ON PROMULGATION OF STANDARDS AND GUIDELINES.—The decision by the Secretary of Commerce regarding the promulgation of any standard or guideline under this section shall occur not later than 6 months after the date of submission of the proposed standard to the Secretary of Commerce by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

''(f) NOTICE AND COMMENT.—A decision by the Secretary of Commerce to significantly modify, or not promulgate, a proposed standard submitted to the Secretary by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) shall be made after the public is given an opportunity to comment on the Secretary's proposed decision.

''(g) DEFINITIONS.—In this section:

''(1) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' has the meaning given the term in section 3552 of title 44.

''(2) INFORMATION SECURITY.—The term 'information security' has the meaning given the term in section 3552 of title 44.

''(3) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given the term in section 3552 of title 44.''.

SEC. 203. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 204. TECHNICAL AND CONFORMING AMENDMENTS.

Section 21(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4(b)) is amended—

(1) in paragraph (2), by striking ''and the Director of the Office of Management and Budget'' and inserting '', the Secretary of Commerce, and the Secretary of Homeland Security''; and

(2) in paragraph (3), by inserting '', the Secretary of Homeland Security,'' after ''the Secretary of Commerce''.

SEC. 205. CLARIFICATION OF AUTHORITIES.

Nothing in this title shall be construed to convey any new regulatory authority to any government entity implementing or complying with any provision of this title.

TITLE III—CRIMINAL PENALTIES

SEC. 301. PENALTIES FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030(c) of title 18, United States Code, is amended to read as follows:

''(c) The punishment for an offense under subsection (a) or (b) of this section is—

''(1) a fine under this title or imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(1) of this section;

''(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than 3 years, or both, in the case of an offense under subsection (a)(2); or

''(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2) of this section, if—

''(i) the offense was committed for purposes of commercial advantage or private financial gain;

''(ii) the offense was committed in the furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States, or of any State; or

''(iii) the value of the information obtained, or that would have been obtained if the offense was completed, exceeds $5,000;

''(3) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(3) of this section;

''(4) a fine under this title or imprisonment of not more than 20 years, or both, in the case of an offense under subsection (a)(4) of this section;

''(5)(A) except as provided in subparagraph (C), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A) of this section, if the offense caused—

''(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

''(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

''(iii) physical injury to any person;

''(iv) a threat to public health or safety;

''(v) damage affecting a computer used by, or on behalf of, an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

''(vi) damage affecting 10 or more protected computers during any 1-year period;

''(B) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(B), if the offense caused a harm provided in clause (i) through (vi) of subparagraph (A) of this subsection;

''(C) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both;

''(D) a fine under this title, imprisonment for not more than 10 years, or both, for any other offense under subsection (a)(5);

''(E) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(6) of this section; or

''(F) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(7) of this section.''.

SEC. 302. TRAFFICKING IN PASSWORDS.

Section 1030(a)(6) of title 18, United States Code, is amended to read as follows:

''(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information or means of access through which a protected computer (as defined in subparagraphs (A) and (B) of subsection (e)(2)) may be accessed without authorization.''.

SEC. 303. CONSPIRACY AND ATTEMPTED COMPUTER FRAUD OFFENSES.

Section 1030(b) of title 18, United States Code, is amended by inserting ''as if for the completed offense'' after ''punished as provided''.

SEC. 304. CRIMINAL AND CIVIL FORFEITURE FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030 of title 18, United States Code, is amended by striking subsections (i) and (j) and inserting the following:

''(i) CRIMINAL FORFEITURE.—

''(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

''(A) such persons interest in any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of such violation; and

''(B) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of such violation.

''(2) The criminal forfeiture of property under this subsection, including any seizure and disposition of the property, and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse

Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

''(j) CIVIL FORFEITURE.—

''(1) The following shall be subject to forfeiture to the United States and no property right, real or personal, shall exist in them:

''(A) Any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of any violation of this section, or a conspiracy to violate this section.

''(B) Any property, real or personal, constituting or derived from any gross proceeds obtained directly or indirectly, or any property traceable to such property, as a result of the commission of any violation of this section, or a conspiracy to violate this section.

''(2) Seizures and forfeitures under this subsection shall be governed by the provisions in chapter 46 relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents and other persons as may be designated for that purpose by the Secretary of Homeland Security or the Attorney General.''.

SEC. 305. DAMAGE TO CRITICAL INFRASTRUCTURE COMPUTERS.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

''§ 1030A. Aggravated damage to a critical infrastructure computer

''(a) DEFINITIONS.—In this section—

''(1) the term 'computer' has the meaning given the term in section 1030;

''(2) the term 'critical infrastructure computer' means a computer that manages or controls systems or assets vital to national defense, national security, national economic security, public health or safety, or any combination of those matters, whether publicly or privately owned or operated, including—

''(A) oil and gas production, storage, conversion, and delivery systems;

''(B) water supply systems;

''(C) telecommunication networks;

''(D) electrical power generation and delivery systems;

''(E) finance and banking systems;

''(F) emergency services;

''(G) transportation systems and services; and

''(H) government operations that provide essential services to the public; and

''(3) the term 'damage' has the meaning given the term in section 1030.

''(b) OFFENSE.—It shall be unlawful, during and in relation to a felony violation of section 1030, to knowingly cause or attempt to cause damage to a critical infrastructure computer if the damage results in (or, in the case of an attempt, if completed, would have resulted in) the substantial impairment—

''(1) of the operation of the critical infrastructure computer; or

''(2) of the critical infrastructure associated with the computer.

''(c) PENALTY.—Any person who violates subsection (b) shall be—

''(1) fined under this title;

''(2) imprisoned for not less than 3 years but not more than 20 years; or

''(3) penalized under paragraphs (1) and (2).

''(d) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

''(1) a court shall not place on probation any person convicted of a violation of this section;

''(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment, including any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for a felony violation of section 1030;

''(3) in determining any term of imprisonment to be imposed for a felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The chapter analysis for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

''1030A. Aggravated damage to a critical infrastructure computer.''.

SEC. 306. LIMITATION ON ACTIONS INVOLVING UNAUTHORIZED USE.

Section 1030(e)(6) of title 18, United States Code, is amended by striking ''alter;'' and inserting ''alter, but does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized;''.

SEC. 307. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

TITLE IV—CYBERSECURITY RESEARCH AND DEVELOPMENT

SEC. 401. NATIONAL HIGH-PERFORMANCE COMPUTING PROGRAM PLANNING AND COORDINATION.

(a) GOALS AND PRIORITIES.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(d) GOALS AND PRIORITIES.—The goals and priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include—

''(1) encouraging and supporting mechanisms for interdisciplinary research and development in networking and information technology, including—

''(A) through collaborations across agencies;

''(B) through collaborations across Program Component Areas;

''(C) through collaborations with industry;

''(D) through collaborations with institutions of higher education;

''(E) through collaborations with Federal laboratories (as defined in section 4 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3703)); and

''(F) through collaborations with international organizations;

''(2) addressing national, multi-agency, multi-faceted challenges of national importance; and

''(3) fostering the transfer of research and development results into new technologies and applications for the benefit of society.''.

(b) DEVELOPMENT OF STRATEGIC PLAN.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(e) STRATEGIC PLAN.—

''(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the agencies under subsection (a)(3)(B), working through the National Science and Technology Council and with the assistance of the Office of Science and Technology Policy shall develop a 5-year strategic plan to guide the activities under subsection (a)(1).

''(2) CONTENTS.—The strategic plan shall specify—

''(A) the near-term objectives for the Program;

''(B) the long-term objectives for the Program;

''(C) the anticipated time frame for achieving the near-term objectives;

''(D) the metrics that will be used to assess any progress made toward achieving the near-term objectives and the long-term objectives; and

''(E) how the Program will achieve the goals and priorities under subsection (d).

''(3) IMPLEMENTATION ROADMAP.—

''(A) IN GENERAL.—The agencies under subsection (a)(3)(B) shall develop and annually update an implementation roadmap for the strategic plan.

''(B) REQUIREMENTS.—The information in the implementation roadmap shall be coordinated with the database under section 102(c) and the annual report under section 101(a)(3). The implementation roadmap shall—

''(i) specify the role of each Federal agency in carrying out or sponsoring research and development to meet the research objectives of the strategic plan, including a description of how progress toward the research objectives will be evaluated, with consideration of any relevant recommendations of the advisory committee;

''(ii) specify the funding allocated to each major research objective of the strategic plan and the source of funding by agency for the current fiscal year; and

''(iii) estimate the funding required for each major research objective of the strategic plan for the next 3 fiscal years.

''(4) RECOMMENDATIONS.—The agencies under subsection (a)(3)(B) shall take into consideration when developing the strategic plan under paragraph (1) the recommendations of—

''(A) the advisory committee under subsection (b); and

''(B) the stakeholders under section 102(a)(3).

''(5) REPORT TO CONGRESS.—The Director of the Office of Science and Technology Policy shall transmit the strategic plan under this subsection, including the implementation roadmap and any updates under paragraph (3), to—

''(A) the advisory committee under subsection (b);

''(B) the Committee on Commerce, Science, and Transportation of the Senate; and

''(C) the Committee on Science and Technology of the House of Representatives.''.

(c) PERIODIC REVIEWS.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(f) PERIODIC REVIEWS.—The agencies under subsection (a)(3)(B) shall—

''(1) periodically assess the contents and funding levels of the Program Component Areas and restructure the Program when warranted, taking into consideration any relevant recommendations of the advisory committee under subsection (b); and

''(2) ensure that the Program includes national, multi-agency, multi-faceted research and development activities, including activities described in section 104.''.

(d) ADDITIONAL RESPONSIBILITIES OF DIRECTOR.—Section 101(a)(2) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(2)) is amended—

(1) by redesignating subparagraphs (E) and (F) as subparagraphs (G) and (H), respectively; and

(2) by inserting after subparagraph (D) the following:

''(E) encourage and monitor the efforts of the agencies participating in the Program to allocate the level of resources and management attention necessary—

''(i) to ensure that the strategic plan under subsection (e) is developed and executed effectively; and

''(ii) to ensure that the objectives of the Program are met;

''(F) working with the Office of Management and Budget and in coordination with the creation of the database under section 102(c), direct the Office of Science and Technology Policy and the agencies participating in the Program to establish a mechanism (consistent with existing law) to track all ongoing and completed research and development projects and associated funding;''.

(e) ADVISORY COMMITTEE.—Section 101(b) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(b)) is amended—

(1) in paragraph (1)—

(A) by inserting after the first sentence the following: ''The co-chairs of the advisory committee shall meet the qualifications of committee members and may be members of the Presidents Council of Advisors on Science and Technology.''; and

(B) by striking ''high-performance'' in subparagraph (D) and inserting ''high-end''; and

(2) by amending paragraph (2) to read as follows:

''(2) In addition to the duties under paragraph (1), the advisory committee shall conduct periodic evaluations of the funding, management, coordination, implementation, and activities of the Program. The advisory committee shall report its findings and recommendations not less frequently than once every 3 fiscal years to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives. The report shall be submitted in conjunction with the update of the strategic plan.''.

(f) REPORT.—Section 101(a)(3) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(3)) is amended—

(1) in subparagraph (C)—

(A) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(B) by striking ''each Program Component Area'' and inserting ''each Program Component Area and each research area supported in accordance with section 104'';

(2) in subparagraph (D)—

(A) by striking ''each Program Component Area,'' and inserting ''each Program Component Area and each research area supported in accordance with section 104,'';

(B) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(C) by striking ''and'' after the semicolon;

(3) by redesignating subparagraph (E) as subparagraph (G); and

(4) by inserting after subparagraph (D) the following:

''(E) include a description of how the objectives for each Program Component Area, and the objectives for activities that involve multiple Program Component Areas, relate to the objectives of the Program identified in the strategic plan under subsection (e);

''(F) include—

''(i) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the next fiscal year by category of activity;

''(ii) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the current fiscal year by category of activity; and

''(iii) the amount of funding provided for the Office of Science and Technology Policy for the current fiscal year by each agency participating in the Program; and''.

(g) DEFINITIONS.—Section 4 of the High-Performance Computing Act of 1991 (15 U.S.C. 5503) is amended—

(1) by redesignating paragraphs (1) and (2) as paragraphs (2) and (3), respectively;

(2) by redesignating paragraph (3) as paragraph (6);

(3) by redesignating paragraphs (6) and (7) as paragraphs (7) and (8), respectively;

(4) by inserting before paragraph (2), as redesignated, the following:

''(1) 'cyber-physical systems' means physical or engineered systems whose networking and information technology functions and physical elements are deeply integrated and are actively connected to the physical world through sensors, actuators, or other means to perform monitoring and control functions;'';

(5) in paragraph (3), as redesignated, by striking ''high-performance computing'' and inserting ''networking and information technology'';

(6) in paragraph (6), as redesignated—

(A) by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(B) by striking ''supercomputer'' and inserting ''high-end computing'';

(7) in paragraph (5), by striking ''network referred to as'' and all that follows through the semicolon and inserting ''network, including advanced computer networks of Federal agencies and departments''; and

(8) in paragraph (7), as redesignated, by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program''.

SEC. 402. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

(a) RESEARCH IN AREAS OF NATIONAL IMPORTANCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.) is amended by adding at the end the following:

''SEC. 104. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

''(a) IN GENERAL.—The Program shall encourage agencies under section 101(a)(3)(B) to support, maintain, and improve national, multi-agency, multi-faceted, research and development activities in networking and information technology directed toward application areas that have the potential for significant contributions to national economic competitiveness and for other significant societal benefits.

''(b) TECHNICAL SOLUTIONS.—An activity under subsection (a) shall be designed to advance the development of research discoveries by demonstrating technical solutions to important problems in areas including—

''(1) cybersecurity;

''(2) health care;

''(3) energy management and low-power systems and devices;

''(4) transportation, including surface and air transportation;

''(5) cyber-physical systems;

''(6) large-scale data analysis and modeling of physical phenomena;

''(7) large scale data analysis and modeling of behavioral phenomena;

''(8) supply chain quality and security; and

''(9) privacy protection and protected disclosure of confidential data.

''(c) RECOMMENDATIONS.—The advisory committee under section 101(b) shall make recommendations to the Program for candidate research and development areas for support under this section.

''(d) CHARACTERISTICS.—

''(1) IN GENERAL.—Research and development activities under this section—

''(A) shall include projects selected on the basis of applications for support through a competitive, merit-based process;

''(B) shall leverage, when possible, Federal investments through collaboration with related State initiatives;

''(C) shall include a plan for fostering the transfer of research discoveries and the results of technology demonstration activities, including from institutions of higher education and Federal laboratories, to industry for commercial development;

''(D) shall involve collaborations among researchers in institutions of higher education and industry; and

''(E) may involve collaborations among nonprofit research institutions and Federal laboratories, as appropriate.

''(2) COST-SHARING.—In selecting applications for support, the agencies under section 101(a)(3)(B) shall give special consideration to projects that include cost sharing from non-Federal sources.

''(3) MULTIDISCIPLINARY RESEARCH CENTERS.—Research and development activities under this section shall be supported through multidisciplinary research centers, including Federal laboratories, that are organized to investigate basic research questions and carry out technology demonstration activities in areas described in subsection (a). Research may be carried out through existing multidisciplinary centers, including those authorized under section 7024(b)(2) of the America COMPETES Act (42 U.S.C. 1862o–10(2)).''.

(b) CYBER-PHYSICAL SYSTEMS.—Section 101(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following:

''(J) provide for increased understanding of the scientific principles of cyber-physical systems and improve the methods available for the design, development, and operation of cyber-physical systems that are characterized by high reliability, safety, and security; and

''(K) provide for research and development on human-computer interactions, visualization, and big data.''.

(c) TASK FORCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.), as amended by section 402(a) of this Act, is amended by adding at the end the following:

''SEC. 105. TASK FORCE.

''(a) ESTABLISHMENT.—Not later than 180 days after the date of enactment the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy under section 102 shall convene a task force to explore mechanisms for carrying out collaborative research and development activities for cyber-physical systems (including the related technologies required to enable

these systems) through a consortium or other appropriate entity with participants from institutions of higher education, Federal laboratories, and industry.

''(b) FUNCTIONS.—The task force shall—

''(1) develop options for a collaborative model and an organizational structure for such entity under which the joint research and development activities could be planned, managed, and conducted effectively, including mechanisms for the allocation of resources among the participants in such entity for support of such activities;

''(2) propose a process for developing a research and development agenda for such entity, including guidelines to ensure an appropriate scope of work focused on nationally significant challenges and requiring collaboration and to ensure the development of related scientific and technological milestones;

''(3) define the roles and responsibilities for the participants from institutions of higher education, Federal laboratories, and industry in such entity;

''(4) propose guidelines for assigning intellectual property rights and for transferring research results to the private sector; and

''(5) make recommendations for how such entity could be funded from Federal, State, and non-governmental sources.

''(c) COMPOSITION.—In establishing the task force under subsection (a), the Director of the Office of Science and Technology Policy shall appoint an equal number of individuals from institutions of higher education and from industry with knowledge and expertise in cyber-physical systems, and may appoint not more than 2 individuals from Federal laboratories.

''(d) REPORT.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy shall transmit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives a report describing the findings and recommendations of the task force.

''(e) TERMINATION.—The task force shall terminate upon transmittal of the report required under subsection (d).

''(f) COMPENSATION AND EXPENSES.—Members of the task force shall serve without compensation.''.

SEC. 403. PROGRAM IMPROVEMENTS.

Section 102 of the High-Performance Computing Act of 1991 (15 U.S.C. 5512) is amended to read as follows:

''SEC. 102. PROGRAM IMPROVEMENTS.

''(a) FUNCTIONS.—The Director of the Office of Science and Technology Policy shall continue—

''(1) to provide technical and administrative support to—

''(A) the agencies participating in planning and implementing the Program, including support needed to develop the strategic plan under section 101(e); and

''(B) the advisory committee under section 101(b);

''(2) to serve as the primary point of contact on Federal networking and information technology activities for government agencies, academia, industry, professional societies, State computing and networking technology programs, interested citizen groups, and others to exchange technical and programmatic information;

''(3) to solicit input and recommendations from a wide range of stakeholders during the development of each strategic plan under section 101(e) by convening at least 1 workshop with invitees from academia, industry, Federal laboratories, and other relevant organizations and institutions;

''(4) to conduct public outreach, including the dissemination of the advisory committee's findings and recommendations, as appropriate;

''(5) to promote access to and early application of the technologies, innovations, and expertise derived from Program activities to agency missions and systems across the Federal Government and to United States industry;

''(6) to ensure accurate and detailed budget reporting of networking and information technology research and development investment; and

''(7) to encourage agencies participating in the Program to use existing programs and resources to strengthen networking and information technology education and training, and increase participation in such fields, including by women and underrepresented minorities.

''(b) SOURCE OF FUNDING.—

''(1) IN GENERAL.—The functions under this section shall be supported by funds from each agency participating in the Program.

''(2) SPECIFICATIONS.—The portion of the total budget of the Office of Science and Technology Policy that is provided by each agency participating in the Program for each fiscal year shall be in the same proportion as each agency's share of the total budget for the Program for the previous fiscal year, as specified in the database under section 102(c).

''(c) DATABASE.—

''(1) IN GENERAL.—The Director of the Office of Science and Technology Policy shall develop and maintain a database of projects funded by each agency for the fiscal year for each Program Component Area.

''(2) PUBLIC ACCESSIBILITY.—The Director of the Office of Science and Technology Policy shall make the database accessible to the public.

''(3) DATABASE CONTENTS.—The database shall include, for each project in the database—

''(A) a description of the project;

''(B) each agency, industry, institution of higher education, Federal laboratory, or international institution involved in the project;

''(C) the source funding of the project (set forth by agency);

''(D) the funding history of the project; and

''(E) whether the project has been completed.''.

SEC. 404. IMPROVING EDUCATION OF NETWORKING AND INFORMATION TECHNOLOGY, INCLUDING HIGH PERFORMANCE COMPUTING.

Section 201(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)) is amended—

(1) by redesignating paragraphs (2) through (4) as paragraphs (3) through (5), respectively; and

(2) by inserting after paragraph (1) the following:

''(2) the National Science Foundation shall use its existing programs, in collaboration with other agencies, as appropriate, to improve the teaching and learning of networking and information technology at all levels of education and to increase participation in networking and information technology fields;''.

SEC. 405. CONFORMING AND TECHNICAL AMENDMENTS TO THE HIGH-PERFORMANCE COMPUTING ACT OF 1991.

(a) SECTION 3.—Section 3 of the High-Performance Computing Act of 1991 (15 U.S.C. 5502) is amended—

(1) in the matter preceding paragraph (1), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(2) in paragraph (1)—

(A) in the matter preceding subparagraph (A), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(B) in subparagraphs (A), (F), and (G), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(C) in subparagraph (H), by striking ''high-performance'' and inserting ''high-end''; and

(3) in paragraph (2)—

(A) by striking ''high-performance computing and'' and inserting ''networking and information technology, and''; and

(B) by striking ''high-performance computing network'' and inserting ''networking and information technology''.

(b) TITLE HEADING.—The heading of title I of the High-Performance Computing Act of 1991 (105 Stat. 1595) is amended by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''.

(c) SECTION 101.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT**'';

(2) in subsection (a)—

(A) in the subsection heading, by striking ''NATIONAL HIGH-PERFORMANCE COMPUTING'' and inserting ''NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT'';

(B) in paragraph (1)—

(i) by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program'';

(ii) in subparagraph (A), by striking ''high-performance computing, including networking'' and inserting ''networking and information technology'';

(iii) in subparagraphs (B) and (G), by striking ''high-performance'' each place it appears and inserting ''high-end''; and

(iv) in subparagraph (C), by striking ''high-performance computing and networking'' and inserting ''high-end computing, distributed, and networking''; and

(C) in paragraph (2)—

(i) in subparagraphs (A) and (C)—

(I) by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(II) by striking ''development, networking,'' each place it appears and inserting ''development,''; and

(ii) in subparagraphs (G) and (H), as redesignated by section 401(d) of this Act, by striking ''high-performance'' each place it appears and inserting ''high-end'';

(3) in subsection (b)(1), in the matter preceding subparagraph (A), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(4) in subsection (c)(1)(A), by striking ''high-performance computing'' and inserting ''networking and information technology''.

(d) SECTION 201.—Section 201(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)(1)) is amended by striking ''high-performance computing and advanced high-speed computer networking'' and inserting ''networking and information technology research and development''.

(e) SECTION 202.—Section 202(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5522(a)) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(f) SECTION 203.—Section 203(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5523(a)) is amended—

(1) in paragraph (1), by striking ''high-performance computing and networking'' and inserting ''networking and information technology''; and

(2) in paragraph (2)(A), by striking ''high-performance'' and inserting ''high-end''.

(g) SECTION 204.—Section 204 of the High-Performance Computing Act of 1991 (15 U.S.C. 5524) is amended—

(1) in subsection (a)(1)—

(A) in subparagraph (A), by striking ''high-performance computing systems and networks'' and inserting ''networking and information technology systems and capabilities'';

(B) in subparagraph (B), by striking ''interoperability of high-performance computing systems in networks and for common user interfaces to systems'' and inserting ''interoperability and usability of networking and information technology systems''; and

(C) in subparagraph (C), by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(2) in subsection (b)—

(A) by striking ''HIGH-PERFORMANCE COMPUTING AND NETWORK'' in the heading and inserting ''NETWORKING AND INFORMATION TECHNOLOGY''; and

(B) by striking ''sensitive''.

(h) SECTION 205.—Section 205(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5525(a)) is amended by striking ''computational'' and inserting ''networking and information technology''.

(i) SECTION 206.—Section 206(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5526(a)) is amended by striking ''computational research'' and inserting ''networking and information technology research''.

(j) SECTION 207.—Section 207 of the High-Performance Computing Act of 1991 (15 U.S.C. 5527) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(k) SECTION 208.—Section 208 of the High-Performance Computing Act of 1991 (15 U.S.C. 5528) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''; and

(2) in subsection (a)—

(A) in paragraph (1), by striking ''High-performance computing and associated'' and inserting ''Networking and information'';

(B) in paragraph (2), by striking ''high-performance computing'' and inserting ''networking and information technologies'';

(C) in paragraph (3), by striking ''high-performance'' and inserting ''high-end'';

(D) in paragraph (4), by striking ''high-performance computers and associated'' and inserting ''networking and information''; and

(E) in paragraph (5), by striking ''high-performance computing and associated'' and inserting ''networking and information''.

SEC. 406. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation, in coordination with the Secretary of Homeland Security, shall carry out a Federal cyber scholarship-for-service program to recruit and train the next generation of information technology professionals and security managers to meet the needs of the cybersecurity mission for the Federal government.

(b) PROGRAM DESCRIPTION AND COMPONENTS.—The program shall—

(1) annually assess the workforce needs of the Federal government for cybersecurity professionals, including network engineers, software engineers, and other experts in order to determine how many scholarships should be awarded annually to ensure that the workforce needs following graduation match the number of scholarships awarded;

(2) provide scholarships for up to 1,000 students per year in their pursuit of undergraduate or graduate degrees in the cybersecurity field, in an amount that may include coverage for full tuition, fees, and a stipend;

(3) require each scholarship recipient, as a condition of receiving a scholarship under the program, to serve in a Federal information technology workforce for a period equal to one and one-half times each year, or partial year, of scholarship received, in addition to an internship in the cybersecurity field, if applicable, following graduation;

(4) provide a procedure for the National Science Foundation or a Federal agency, consistent with regulations of the Office of Personnel Management, to request and fund a security clearance for a scholarship recipient, including providing for clearance during a summer internship and upon graduation; and

(5) provide opportunities for students to receive temporary appointments for meaningful employment in the Federal information technology workforce during school vacation periods and for internships.

(c) HIRING AUTHORITY.—

(1) IN GENERAL.—For purposes of any law or regulation governing the appointment of an individual in the Federal civil service, upon the successful completion of the student's studies, a student receiving a scholarship under the program may—

(A) be hired under section 213.3102(r) of title 5, Code of Federal Regulations; and

(B) be exempt from competitive service.

(2) COMPETITIVE SERVICE.—Upon satisfactory fulfillment of the service term under paragraph (1), an individual may be converted to a competitive service position without competition if the individual meets the requirements for that position.

(d) ELIGIBILITY.—The eligibility requirements for a scholarship under this section shall include that a scholarship applicant—

(1) be a citizen of the United States;

(2) be eligible to be granted a security clearance;

(3) maintain a grade point average of 3.2 or above on a 4.0 scale for undergraduate study or a 3.5 or above on a 4.0 scale for post-graduate study;

(4) demonstrate a commitment to a career in improving the security of the information infrastructure; and

(5) has demonstrated a level of proficiency in math or computer sciences.

(e) FAILURE TO COMPLETE SERVICE OBLIGATION.—

(1) IN GENERAL.—A scholarship recipient under this section shall be liable to the United States under paragraph (2) if the scholarship recipient—

(A) fails to maintain an acceptable level of academic standing in the educational institution in which the individual is enrolled, as determined by the Director;

(B) is dismissed from such educational institution for disciplinary reasons;

(C) withdraws from the program for which the award was made before the completion of such program;

(D) declares that the individual does not intend to fulfill the service obligation under this section;

(E) fails to fulfill the service obligation of the individual under this section; or

(F) loses a security clearance or becomes ineligible for a security clearance.

(2) REPAYMENT AMOUNTS.—

(A) LESS THAN 1 YEAR OF SERVICE.—If a circumstance under paragraph (1) occurs before the completion of 1 year of a service obligation under this section, the total amount of awards received by the individual under this section shall be repaid.

(B) ONE OR MORE YEARS OF SERVICE.—If a circumstance described in subparagraph (D) or (E) of paragraph (1) occurs after the completion of 1 year of a service obligation under this section, the total amount of scholarship awards received by the individual under this section, reduced by the ratio of the number of years of service completed divided by the number of years of service required, shall be repaid.

(f) EVALUATION AND REPORT.—The Director of the National Science Foundation shall—

(1) evaluate the success of recruiting individuals for scholarships under this section and of hiring and retaining those individuals in the public sector workforce, including the annual cost and an assessment of how the program actually improves the Federal workforce; and

(2) periodically report the findings under paragraph (1) to Congress.

(g) AUTHORIZATION OF APPROPRIATIONS.—From amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), the Secretary may use funds to carry out the requirements of this section for fiscal years 2012 through 2013.

SEC. 407. STUDY AND ANALYSIS OF CERTIFICATION AND TRAINING OF INFORMATION INFRASTRUCTURE PROFESSIONALS.

(a) STUDY.—The President shall enter into an agreement with the National Academies to conduct a comprehensive study of government, academic, and private-sector accreditation, training, and certification programs for personnel working in information infrastructure. The agreement shall require the National Academies to consult with sector coordinating councils and relevant governmental agencies, regulatory entities, and nongovernmental organizations in the course of the study.

(b) SCOPE.—The study shall include—

(1) an evaluation of the body of knowledge and various skills that specific categories of personnel working in information infrastructure should possess in order to secure information systems;

(2) an assessment of whether existing government, academic, and private-sector accreditation, training, and certification programs provide the body of knowledge and various skills described in paragraph (1);

(3) an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity talent, including barriers relating to compensation, the hiring process, job classification, and hiring flexibility; and

(4) an analysis of the sources and availability of cybersecurity talent, a comparison of the skills and expertise sought by the Federal Government and the private sector, an examination of the current and future capacity of United States institutions of higher education, including community colleges, to provide current and future cybersecurity professionals, through education and training activities, with those skills sought by the Federal Government, State and local entities, and the private sector.

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the National Academies shall submit to the President and Congress a report on the results of the study. The report shall include—

(1) findings regarding the state of information infrastructure accreditation, training, and certification programs, including specific areas of deficiency and demonstrable progress; and

(2) recommendations for the improvement of information infrastructure accreditation, training, and certification programs.

SEC. 408. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

(a) IN GENERAL.—The Director of the National Institute of Standards and Technology, in coordination with appropriate Federal authorities, shall—

(1) as appropriate, ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to Congress a plan for ensuring such Federal agency coordination.

(b) CONSULTATION WITH THE PRIVATE SECTOR.—In carrying out the activities under subsection (a)(1), the Director shall ensure consultation with appropriate private sector stakeholders.

SEC. 409. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

The Director of the National Institute of Standards and Technology shall continue a program to support the development of technical standards, metrology, testbeds, and conformance criteria, taking into account appropriate user concerns—

(1) to improve interoperability among identity management technologies;

(2) to strengthen authentication methods of identity management systems;

(3) to improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols; and

(4) to improve the usability of identity management systems.

SEC. 410. FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY RESEARCH GRANT AREAS.—Section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking ''property.'' and inserting ''property;''; and

(3) by adding at the end the following:

''(J) secure fundamental protocols that are at the heart of inter-network communications and data exchange;

''(K) system security that addresses the building of secure systems from trusted and untrusted components;

''(L) monitoring and detection; and

''(M) resiliency and rapid recovery methods.''.

(b) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY GRANTS.—Section 4(a)(3) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(3)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Secretary finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(c) COMPUTER AND NETWORK SECURITY CENTERS.—Section 4(b)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7403(b)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Secretary finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(d) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—Section 5(a)(6) of the Cyber Security Research and Development Act (15 U.S.C. 7404(a)(6)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Secretary finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT GRANTS.—Section 5(b)(2) of the Cyber Security Research and Development Act (15 U.S.C. 7404(b)(2)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Secretary finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(f) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY RESEARCH.—Section 5(c)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7404(c)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Secretary finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

SA 2583. Mr. GRASSLEY submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 192, strike line 11 and all that follows through page 193, line 22.

SA 2584. Mr. GRASSLEY submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 18, strike line 16 and all that follows through page 19, line 2, and insert the following:

(5) LIMITATION.—The Council may not identify critical infrastructure as a category of critical cyber infrastructure under this section based solely on activities protected by the first amendment to the Constitution of the United States.

SA 2585. Mr. GRASSLEY submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE VIII—CRIMINAL PENALTIES

SEC. 801. PENALTIES FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030(c) of title 18, United States Code, is amended to read as follows:

''(c) The punishment for an offense under subsection (a) or (b) of this section is—

''(1) a fine under this title or imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(1) of this section;

''(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than 3 years, or both, in the case of an offense under subsection (a)(2); or

''(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2) of this section, if—

''(i) the offense was committed for purposes of commercial advantage or private financial gain;

''(ii) the offense was committed in the furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States, or of any State; or

''(iii) the value of the information obtained, or that would have been obtained if the offense was completed, exceeds $5,000;

''(3) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(3) of this section;

''(4) a fine under this title or imprisonment of not more than 20 years, or both, in the case of an offense under subsection (a)(4) of this section; and

''(5)(A) except as provided in subparagraph (C), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A) of this section, if the offense caused—

''(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

''(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

''(iii) physical injury to any person;

''(iv) a threat to public health or safety;

''(v) damage affecting a computer used by, or on behalf of, an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

''(vi) damage affecting 10 or more protected computers during any 1-year period;

''(B) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(B), if the offense caused a harm described in clause (i) through (vi) of subparagraph (A) of this subsection;

''(C) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both;

''(D) a fine under this title, imprisonment for not more than 10 years, or both, for any other offense under subsection (a)(5);

''(E) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(6) of this section; or

''(F) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(7) of this section.''.

SEC. 802. TRAFFICKING IN PASSWORDS.

Section 1030(a)(6) of title 18, United States Code, is amended to read as follows:

''(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information or means of access through which a protected computer (as defined in subparagraphs (A) and (B) of subsection (e)(2)) may be accessed without authorization; or''.

SEC. 803. CONSPIRACY AND ATTEMPTED COMPUTER FRAUD OFFENSES.

Section 1030(b) of title 18, United States Code, is amended by inserting ''as if for the

completed offense'' after ''punished as provided''.

SEC. 804. CRIMINAL AND CIVIL FORFEITURE FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030 of title 18, United States Code, is amended by striking subsections (i) and (j) and inserting the following:

''(i) CRIMINAL FORFEITURE.—

''(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

''(A) such person's interest in any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of such violation; and

''(B) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of such violation.

''(2) The criminal forfeiture of property under this subsection, including any seizure and disposition of the property, and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

''(j) CIVIL FORFEITURE.—

''(1) The following shall be subject to forfeiture to the United States and no property right, real or personal, shall exist in them:

''(A) Any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of any violation of this section, or a conspiracy to violate this section.

''(B) Any property, real or personal, constituting or derived from any gross proceeds obtained directly or indirectly, or any property traceable to such property, as a result of the commission of any violation of this section, or a conspiracy to violate this section.

''(2) Seizures and forfeitures under this subsection shall be governed by the provisions in chapter 46 relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents and other persons as may be designated for that purpose by the Secretary of Homeland Security or the Attorney General.''.

SEC. 805. DAMAGE TO CRITICAL INFRASTRUCTURE COMPUTERS.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

''§ 1030A. Aggravated damage to a critical infrastructure computer

''(a) DEFINITIONS.—In this section—

''(1) the term 'computer' has the meaning given the term in section 1030;

''(2) the term 'critical infrastructure computer' means a computer that manages or controls systems or assets vital to national defense, national security, national economic security, public health or safety, or any combination of those matters, whether publicly or privately owned or operated, including—

''(A) oil and gas production, storage, conversion, and delivery systems;

''(B) water supply systems;

''(C) telecommunication networks;

''(D) electrical power generation and delivery systems;

''(E) finance and banking systems;

''(F) emergency services;

''(G) transportation systems and services; and

''(H) government operations that provide essential services to the public; and

''(3) the term 'damage' has the meaning given the term in section 1030.

''(b) OFFENSE.—It shall be unlawful, during and in relation to a felony violation of section 1030, to knowingly cause or attempt to cause damage to a critical infrastructure computer if the damage results in (or, in the case of an attempt, if completed, would have resulted in) the substantial impairment—

''(1) of the operation of the critical infrastructure computer; or

''(2) of the critical infrastructure associated with the computer.

''(c) PENALTY.—Any person who violates subsection (b) shall be fined under this title, imprisoned for not less than 3 years but not more than 20 years, or both.

''(d) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

''(1) a court shall not place on probation any person convicted of a violation of this section;

''(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment, including any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for a felony violation of section 1030;

''(3) in determining any term of imprisonment to be imposed for a felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The chapter analysis for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

''1030A. Aggravated damage to a critical infrastructure computer.''.

SEC. 806. LIMITATION ON ACTIONS INVOLVING UNAUTHORIZED USE.

Section 1030(e)(6) of title 18, United States Code, is amended by striking ''alter;'' and inserting ''alter, but does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized;''.

SEC. 807. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SA 2586. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 22, strike lines 8 through 18.

SA 2587. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 30, after line 24, add the following:

(C) RULE OF CONSTRUCTION.—Nothing in this paragraph shall be construed to establish a civil cause of action, or a presumption of negligence in a civil action, against an owner that does not participate in the Voluntary Cybersecurity Program for Critical Infrastructure established under this section.

SA 2588. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 22, line 10, strike ''fails'' and all that follows through line 18 and insert ''chooses not to propose to the Council cybersecurity practices under subsection (a), not later than 180 days after the date of enactment of this Act the sector coordinating council shall submit a report to the Council explaining why it chose not to propose cybersecurity practices.''.

SA 2589. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 30, line 8, after ''106'' insert the following: ''and may not be used for other regulatory purposes by the Federal Government or a State or local government''.

SA 2590. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 21, strike line 8 and all that follows through page 22, line 7, and insert the following:

(B) review relevant regulations or compulsory standards or guidelines; and

(C) review cybersecurity practices proposed under subsection (a) to ensure sufficient protection against cyber risks.

(2) ADOPTION.—

(A) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Council shall—

(i) adopt any cybersecurity practices proposed under subsection (a) that adequately remediate or mitigate identified cyber risks and any associated consequences identified through an assessment conducted under section 102(a); and

(ii) conduct a cost-benefit analysis in accordance with Executive Order 13563 (5 U.S.C. 601 note; relating to improving regulation and regulatory review), including sections 1 and 3 of such Executive Order.

SA 2591. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 16, line 8, after ''mechanism'' insert '', under which it shall be unlawful for

the Federal Government to compel participation,''.

SA 2592. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Strike title IV.

SA 2593. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 10, line 12, after ''shall'' insert the following: ''designate a Federal agency subject to full congressional oversight to''.

SA 2594. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 20, line 2, after ''paragraph (1).'' insert the following: ''If Congress passes a resolution of disapproval of the identification of a category of critical infrastructure as critical cyber infrastructure, the category shall be removed from the list of identified categories of critical cyber infrastructure and may not be identified as a category of critical cyber infrastructure during the 2 year period beginning on the date on which Congress passes the resolution of disapproval.''.

SA 2595. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 23, strike line 22 and all that follows through page 24, line 13, and insert the following:

critical infrastructure may not adopt the cybersecurity practices as mandatory requirements.

(B) RULE OF CONSTRUCTION.—Nothing in

SA 2596. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 13, line 11, insert ''In addition, any authority of a Federal agency under another provision of law to compel owners or operators to provide information to the Federal Government may not be used in furtherance of this Act.'' after the period.

SA 2597. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Strike title I.

SA 2598. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 16, line 21, strike ''and''.

On page 16, line 23, strike the period and insert ''; and''.

On page 16, between lines 23 and 24, insert the following:

(H) submit to the President and the appropriate congressional committees a report, which may be in classified or unclassified form, explaining the methodologies use to identify and results of the identification of categories of critical cyber infrastructure.

SA 2599. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 24, strike lines 3 through 12 and insert the following:

adopted the cybersecurity practices as mandatory requirements, the Federal agency shall submit to the appropriate congressional committees a report on the reasons the Federal agency did so, including an explanation of how the Federal agency conducted a detailed cost-benefit analysis in accordance with Executive Order 13563 (5 U.S.C. 601 note; relating to improving regulation and regulatory review), including sections 1 and 3 of such Executive Order.

SA 2600. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 18, strike line 18 and all that follows through page 19, line 2, and insert the following: ''under this section critical infrastructure based solely on activities protected by the first amendment to the Constitution of the United States.''.

SA 2601. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 34, strike lines 3 through 19 and insert the following:

(1) provide additional authority for any sector-specific agency or any Federal agency that is not a sector-specific agency with responsibilities for regulating the security of critical infrastructure to establish standards or other cybersecurity measures that are applicable to the security of critical infrastructure not otherwise authorized by law;

(2) limit or restrict the authority of the Department, or any other Federal agency, under any other provision of law; or

(3) permit any owner (including a certified owner) to fail to comply with any other law or regulation, unless specifically authorized.

SA 2602. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 173, beginning on line 14, strike ''The Secretary of Homeland Security, in consultation with'' and insert ''The President, in consultation with the Secretary,''.

On page 173, line 19, strike ''civilian''.

On page 174, line 11, strike ''CIVILIAN''.

On page 174, beginning on line 13, strike ''The Secretary, in consultation with'' and insert ''The President, in consultation with the Secretary,''.

On page 174, line 16, strike ''civilian''.

On page 174, beginning on line 21, strike ''civilian''.

On page 177, line 2, strike ''civilian''.

On page 177, line 6, strike ''CIVILIAN''.

On page 177, beginning on line 8, strike ''the Secretary, in consultation with'' and insert ''the President, in consultation with the Secretary,''.

On page 177, line 11, strike ''civilian''.

On page 177, line 23, strike ''the Secretary'' and insert ''the President''.

On page 178, line 21, strike ''The Secretary'' and insert ''The President''.

On page 179, beginning on line 6, strike ''The Secretary, in coordination with the Director of National Intelligence, the Attorney General, and the Secretary of Defense,'' and insert ''The President''.

On page 183, beginning on line 15, strike ''the Secretary and approved by the Attorney General'' and insert ''the President''.

On page 184, beginning on line 19, strike ''The Secretary, in consultation with privacy and civil liberties experts,'' and insert ''The President, in consultation with privacy and civil liberties experts, the Secretary,''.

On page 186, strike lines 16 through 22.

On page 186, line 24, strike ''The Secretary'' and insert ''The President''.

On page 187, beginning on line 10, strike ''The Secretary and the Attorney General'' and insert ''The President, in consultation with the Secretary and the Attorney General,''.

On page 187, beginning on line 20, strike ''the Secretary and approved by the Attorney General'' and insert ''the President''.

On page 187, beginning on line 23, strike ''the Attorney General'' and insert ''the President''.

On page 188, line 1, strike ''the Attorney General'' and insert ''the President''.

On page 188, line 3, strike ''the Attorney General'' and insert ''the President''.

On page 202, beginning on line 21, strike ''the Secretary, the Director of National Intelligence, the Attorney General, and the Secretary of Defense shall jointly'' and insert ''the President, in consultation with the Secretary, the Director of National Intelligence, the Attorney General, and the Secretary of Defense, shall''.

SA 2603. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 173, beginning on line 14, strike ''The Secretary of Homeland Security, in consultation with'' and insert ''The President, in consultation with the Secretary,''.

On page 173, line 19, strike ''civilian''.

On page 174, line 11, strike ''CIVILIAN''.

On page 174, beginning on line 13, strike ''The Secretary, in consultation with'' and insert ''The President, in consultation with the Secretary,''.

On page 174, line 16, strike ''civilian''.

On page 174, beginning on line 21, strike ''civilian''.

On page 177, line 2, strike ''civilian''.

On page 177, line 6, strike ''CIVILIAN''.

On page 177, beginning on line 8, strike ''the Secretary, in consultation with'' and

insert ''the President, in consultation with the Secretary,''.

On page 177, line 11, strike ''civilian''.

On page 177, line 23, strike ''the Secretary'' and insert ''the President''.

On page 178, line 21, strike ''The Secretary'' and insert ''The President''.

On page 179, beginning on line 6, strike ''The Secretary, in coordination with the Director of National Intelligence, the Attorney General, and the Secretary of Defense,'' and insert ''The President''.

On page 183, beginning on line 15, strike ''the Secretary and approved by the Attorney General'' and insert ''the President''.

On page 184, beginning on line 19, strike ''The Secretary, in consultation with privacy and civil liberties experts,'' and insert ''The President, in consultation with privacy and civil liberties experts, the Secretary,''.

On page 186, strike lines 16 through 22.

On page 186, line 24, strike ''The Secretary'' and insert ''The President''.

On page 187, beginning on line 10, strike ''The Secretary and the Attorney General'' and insert ''The President, in consultation with the Secretary and the Attorney General,''.

On page 187, beginning on line 20, strike ''the Secretary and approved by the Attorney General'' and insert ''the President''.

On page 187, beginning on line 23, strike ''the Attorney General'' and insert ''the President''.

On page 188, line 1, strike ''the Attorney General'' and insert ''the President''.

On page 188, line 3, strike ''the Attorney General'' and insert ''the President''.

On page 199, strike lines 12 through 17.

On page 202, beginning on line 21, strike ''the Secretary, the Director of National Intelligence, the Attorney General, and the Secretary of Defense shall jointly'' and insert ''the President, in consultation with the Secretary, the Director of National Intelligence, the Attorney General, and the Secretary of Defense, shall''.

SA 2604. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of title I, add the following:

SEC. 111. SUNSET.

This title is repealed effective on the date that is 4 years after the date of enactment of this Act.

SA 2605. Mr. MCCAIN (for himself, Mrs. HUTCHISON, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012'' or ''SECURE IT''.

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

TITLE I—FACILITATING SHARING OF CYBER THREAT INFORMATION

SEC. 101. DEFINITIONS.

In this title:

(1) AGENCY.—The term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code.

(2) ANTITRUST LAWS.—The term ''antitrust laws''—

(A) has the meaning given the term in section 1(a) of the Clayton Act (15 U.S.C. 12(a));

(B) includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that section 5 of that Act applies to unfair methods of competition; and

(C) includes any State law that has the same intent and effect as the laws under subparagraphs (A) and (B).

(3) COUNTERMEASURE.—The term ''countermeasure'' means an automated or a manual action with defensive intent to mitigate cyber threats.

(4) CYBER THREAT INFORMATION.—The term ''cyber threat information'' means information that indicates or describes—

(A) a technical or operation vulnerability or a cyber threat mitigation measure;

(B) an action or operation to mitigate a cyber threat;

(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

(D) a method of defeating a technical control;

(E) a method of defeating an operational control;

(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

(G) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to inadvertently enable the defeat of a technical or operational control;

(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

(J) any combination of subparagraphs (A) through (I).

(5) CYBERSECURITY CENTER.—The term ''cybersecurity center'' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

(6) CYBERSECURITY SYSTEM.—The term ''cybersecurity system'' means a system designed or employed to ensure the integrity, confidentiality, or availability of, or to safeguard, a system or network, including measures intended to protect a system or network from—

(A) efforts to degrade, disrupt, or destroy such system or network; or

(B) theft or misappropriations of private or government information, intellectual property, or personally identifiable information.

(7) ENTITY.—

(A) IN GENERAL.—The term ''entity'' means any private entity, non-Federal government agency or department, or State, tribal, or local government agency or department (including an officer, employee, or agent thereof).

(B) INCLUSIONS.—The term ''entity'' includes a government agency or department (including an officer, employee, or agent thereof) of the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States.

(8) FEDERAL INFORMATION SYSTEM.—The term ''Federal information system'' means an information system of a Federal department or agency used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

(9) INFORMATION SECURITY.—The term ''information security'' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; or

(C) availability, by ensuring timely and reliable access to and use of information.

(10) INFORMATION SYSTEM.—The term ''information system'' has the meaning given the term in section 3502 of title 44, United States Code.

(11) LOCAL GOVERNMENT.—The term ''local government'' means any borough, city, county, parish, town, township, village, or other general purpose political subdivision of a State.

(12) MALICIOUS RECONNAISSANCE.—The term ''malicious reconnaissance'' means a method for actively probing or passively monitoring an information system for the purpose of discerning technical vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(13) OPERATIONAL CONTROL.—The term ''operational control'' means a security control for an information system that primarily is implemented and executed by people.

(14) OPERATIONAL VULNERABILITY.—The term ''operational vulnerability'' means any attribute of policy, process, or procedure that could enable or facilitate the defeat of an operational control.

(15) PRIVATE ENTITY.—The term ''private entity'' means any individual or any private group, organization, or corporation, including an officer, employee, or agent thereof.

(16) SIGNIFICANT CYBER INCIDENT.—The term ''significant cyber incident'' means a cyber incident resulting in, or an attempted cyber incident that, if successful, would have resulted in—

(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

(17) TECHNICAL CONTROL.—The term ''technical control'' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

(18) TECHNICAL VULNERABILITY.—The term ''technical vulnerability'' means any attribute of hardware or software that could enable or facilitate the defeat of a technical control.

(19) TRIBAL.—The term ''tribal'' has the meaning given the term ''Indian tribe'' in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

SEC. 102. AUTHORIZATION TO SHARE CYBER THREAT INFORMATION.

(a) VOLUNTARY DISCLOSURE.—

(1) PRIVATE ENTITIES.—Notwithstanding any other provision of law, a private entity may, for the purpose of preventing, investigating, or otherwise mitigating threats to information security, on its own networks, or as authorized by another entity, on such entity's networks, employ countermeasures and use cybersecurity systems in order to obtain, identify, or otherwise possess cyber threat information.

(2) ENTITIES.—Notwithstanding any other provision of law, an entity may disclose cyber threat information to—

(A) a cybersecurity center; or

(B) any other entity in order to assist with preventing, investigating, or otherwise mitigating threats to information security.

(3) INFORMATION SECURITY PROVIDERS.—If the cyber threat information described in paragraph (1) is obtained, identified, or otherwise possessed in the course of providing information security products or services under contract to another entity, that entity shall be given, at any time prior to disclosure of such information, a reasonable opportunity to authorize or prevent such disclosure, to request anonymization of such information, or to request that reasonable efforts be made to safeguard such information that identifies specific persons from unauthorized access or disclosure.

(b) SIGNIFICANT CYBER INCIDENTS INVOLVING FEDERAL INFORMATION SYSTEMS.—

(1) IN GENERAL.—An entity providing electronic communication services, remote computing services, or information security services to a Federal department or agency shall inform the Federal department or agency of a significant cyber incident involving the Federal information system of that Federal department or agency that—

(A) is directly known to the entity as a result of providing such services;

(B) is directly related to the provision of such services by the entity; and

(C) as determined by the entity, has impeded or will impede the performance of a critical mission of the Federal department or agency.

(2) ADVANCE COORDINATION.—A Federal department or agency receiving the services described in paragraph (1) shall coordinate in advance with an entity described in paragraph (1) to develop the parameters of any information that may be provided under paragraph (1), including clarification of the type of significant cyber incident that will impede the performance of a critical mission of the Federal department or agency.

(3) REPORT.—A Federal department or agency shall report information provided under this subsection to a cybersecurity center.

(4) CONSTRUCTION.—Any information provided to a cybersecurity center under paragraph (3) shall be treated in the same manner as information provided to a cybersecurity center under subsection (a).

(c) INFORMATION SHARED WITH OR PROVIDED TO A CYBERSECURITY CENTER.—Cyber threat information provided to a cybersecurity center under this section—

(1) may be disclosed to, retained by, and used by, consistent with otherwise applicable Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal government for a cybersecurity purpose, a national security purpose, or in order to prevent, investigate, or prosecute any of the offenses listed in section 2516 of title 18, United States Code, and such information shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under this paragraph;

(2) may, with the prior written consent of the entity submitting such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(3) shall be considered the commercial, financial, or proprietary information of the entity providing such information to the Federal government and any disclosure outside the Federal government may only be made upon the prior written consent by such entity and shall not constitute a waiver of any applicable privilege or protection provided by law, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(4) shall be deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records;

(5) shall be, without discretion, withheld from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records;

(6) shall not be subject to the rules of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official;

(7) shall not, if subsequently provided to a State, tribal, or local government or government agency, otherwise be disclosed or distributed to any entity by such State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent; and

(8) shall not be directly used by any Federal, State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph.

(d) PROCEDURES RELATING TO INFORMATION SHARING WITH A CYBERSECURITY CENTER.—Not later than 60 days after the date of enactment of this Act, the heads of each department or agency containing a cybersecurity center shall jointly develop, promulgate, and submit to Congress procedures to ensure that cyber threat information shared with or provided to—

(1) a cybersecurity center under this section—

(A) may be submitted to a cybersecurity center by an entity, to the greatest extent possible, through a uniform, publicly available process or format that is easily accessible on the website of such cybersecurity center, and that includes the ability to provide relevant details about the cyber threat information and written consent to any subsequent disclosures authorized by this paragraph;

(B) shall immediately be further shared with each cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government;

(C) is handled by the Federal government in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title, and the Federal government may undertake efforts consistent with this subparagraph to limit the impact on privacy and civil liberties of the sharing of cyber threat information with the Federal government; and

(D) except as provided in this section, shall only be used, disclosed, or handled in accordance with the provisions of subsection (c); and

(2) a Federal agency or department under subsection (b) is provided immediately to a cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to

information security across the Federal government.

(e) INFORMATION SHARED BETWEEN ENTITIES.—

(1) IN GENERAL.—An entity sharing cyber threat information with another entity under this title may restrict the use or sharing of such information by such other entity.

(2) FURTHER SHARING.—Cyber threat information shared by any entity with another entity under this title—

(A) shall only be further shared in accordance with any restrictions placed on the sharing of such information by the entity authorizing such sharing, such as appropriate anonymization of such information; and

(B) may not be used by any entity to gain an unfair competitive advantage to the detriment of the entity authorizing the sharing of such information, except that the conduct described in paragraph (3) shall not constitute unfair competitive conduct.

(3) INFORMATION SHARED WITH STATE, TRIBAL, OR LOCAL GOVERNMENT OR GOVERNMENT AGENCY.—Cyber threat information shared with a State, tribal, or local government or government agency under this title—

(A) may, with the prior written consent of the entity sharing such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent;

(B) shall be deemed voluntarily shared information and exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records;

(C) shall not be disclosed or distributed to any entity by the State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent; and

(D) shall not be directly used by any State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this subparagraph.

(4) ANTITRUST EXEMPTION.—The exchange or provision of cyber threat information or assistance between 2 or more private entities under this title shall not be considered a violation of any provision of antitrust laws if exchanged or provided in order to assist with—

(A) facilitating the prevention, investigation, or mitigation of threats to information security; or

(B) communicating or disclosing of cyber threat information to help prevent, investigate or otherwise mitigate the effects of a threat to information security.

(5) NO RIGHT OR BENEFIT.—The provision of cyber threat information to an entity under this section shall not create a right or a benefit to similar information by such entity or any other entity.

(f) FEDERAL PREEMPTION.—

(1) IN GENERAL.—This section supersedes any statute or other law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this section.

(2) STATE LAW ENFORCEMENT.—Nothing in this section shall be construed to supersede any statute or other law of a State or political subdivision of a State concerning the use of authorized law enforcement techniques.

(3) PUBLIC DISCLOSURE.—No information shared with or provided to a State, tribal, or local government or government agency pursuant to this section shall be made publicly available pursuant to any State, tribal, or local law requiring disclosure of information or records.

(g) CIVIL AND CRIMINAL LIABILITY.—

(1) GENERAL PROTECTIONS.—

(A) PRIVATE ENTITIES.—No cause of action shall lie or be maintained in any court against any private entity for—

(i) the use of countermeasures and cybersecurity systems as authorized by this title;

(ii) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(iii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such private entity.

(B) ENTITIES.—No cause of action shall lie or be maintained in any court against any entity for—

(i) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(ii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such entity.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed as creating any immunity against, or otherwise affecting, any action brought by the Federal government, or any agency or department thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, and use of classified information.

(h) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this section shall be construed to limit or prohibit otherwise lawful disclosures of communications, records, or other information by a private entity to any other governmental or private entity not covered under this section.

(i) WHISTLEBLOWER PROTECTION.—Nothing in this Act shall be construed to preempt or preclude any employee from exercising rights currently provided under any whistleblower law, rule, or regulation.

(j) RELATIONSHIP TO OTHER LAWS.—The submission of cyber threat information under this section to a cybersecurity center shall not affect any requirement under any other provision of law for an entity to provide information to the Federal government.

SEC. 103. INFORMATION SHARING BY THE FEDERAL GOVERNMENT.

(a) CLASSIFIED INFORMATION.—

(1) PROCEDURES.—Consistent with the protection of intelligence sources and methods, and as otherwise determined appropriate, the Director of National Intelligence and the Secretary of Defense, in consultation with the heads of the appropriate Federal departments or agencies, shall develop and promulgate procedures to facilitate and promote—

(A) the immediate sharing, through the cybersecurity centers, of classified cyber threat information in the possession of the Federal government with appropriately cleared representatives of any appropriate entity; and

(B) the declassification and immediate sharing, through the cybersecurity centers, with any entity or, if appropriate, public availability of cyber threat information in the possession of the Federal government;

(2) HANDLING OF CLASSIFIED INFORMATION.—The procedures developed under paragraph (1) shall ensure that each entity receiving classified cyber threat information pursuant to this section has acknowledged in writing the ongoing obligation to comply with all laws, executive orders, and procedures concerning the appropriate handling, disclosure, or use of classified information.

(b) UNCLASSIFIED CYBER THREAT INFORMATION.—The heads of each department or agency containing a cybersecurity center shall jointly develop and promulgate procedures that ensure that, consistent with the provisions of this section, unclassified, including controlled unclassified, cyber threat information in the possession of the Federal government—

(1) is shared, through the cybersecurity centers, in an immediate and adequate manner with appropriate entities; and

(2) if appropriate, is made publicly available.

(c) DEVELOPMENT OF PROCEDURES.—

(1) IN GENERAL.—The procedures developed under this section shall incorporate, to the greatest extent possible, existing processes utilized by sector specific information sharing and analysis centers.

(2) COORDINATION WITH ENTITIES.—In developing the procedures required under this section, the Director of National Intelligence and the heads of each department or agency containing a cybersecurity center shall coordinate with appropriate entities to ensure that protocols are implemented that will facilitate and promote the sharing of cyber threat information by the Federal government.

(d) ADDITIONAL RESPONSIBILITIES OF CYBERSECURITY CENTERS.—Consistent with section 102, a cybersecurity center shall—

(1) facilitate information sharing, interaction, and collaboration among and between cybersecurity centers and—

(A) other Federal entities;

(B) any entity; and

(C) international partners, in consultation with the Secretary of State;

(2) disseminate timely and actionable cybersecurity threat, vulnerability, mitigation, and warning information, including alerts, advisories, indicators, signatures, and mitigation and response measures, to improve the security and protection of information systems; and

(3) coordinate with other Federal entities, as appropriate, to integrate information from across the Federal government to provide situational awareness of the cybersecurity posture of the United States.

(e) SHARING WITHIN THE FEDERAL GOVERNMENT.—The heads of appropriate Federal departments and agencies shall ensure that cyber threat information in the possession of such Federal departments or agencies that relates to the prevention, investigation, or mitigation of threats to information security across the Federal government is shared effectively with the cybersecurity centers.

(f) SUBMISSION TO CONGRESS.—Not later than 60 days after the date of enactment of this Act, the Director of National Intelligence, in coordination with the appropriate head of a department or an agency containing a cybersecurity center, shall submit the procedures required by this section to Congress.

SEC. 104. CONSTRUCTION.

(a) INFORMATION SHARING RELATIONSHIPS.—Nothing in this title shall be construed—

(1) to limit or modify an existing information sharing relationship;

(2) to prohibit a new information sharing relationship;

(3) to require a new information sharing relationship between any entity and the Federal government, except as specified under section 102(b); or

(4) to modify the authority of a department or agency of the Federal government

to protect sources and methods and the national security of the United States.

(b) ANTI-TASKING RESTRICTION.—Nothing in this title shall be construed to permit the Federal government—

(1) to require an entity to share information with the Federal government, except as expressly provided under section 102(b); or

(2) to condition the sharing of cyber threat information with an entity on such entity's provision of cyber threat information to the Federal government.

(c) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this title shall be construed to subject any entity to liability for choosing not to engage in the voluntary activities authorized under this title.

(d) USE AND RETENTION OF INFORMATION.—Nothing in this title shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal government to retain or use any information shared under section 102 for any use other than a use permitted under subsection 102(c)(1).

(e) NO NEW FUNDING.—An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 105. REPORT ON IMPLEMENTATION.

(a) CONTENT OF REPORT.—Not later than 1 year after the date of enactment of this Act, and biennially thereafter, the heads of each department or agency containing a cybersecurity center shall jointly submit, in coordination with the privacy and civil liberties officials of such departments or agencies and the Privacy and Civil Liberties Oversight Board, a detailed report to Congress concerning the implementation of this title, including—

(1) an assessment of the sufficiency of the procedures developed under section 103 of this Act in ensuring that cyber threat information in the possession of the Federal government is provided in an immediate and adequate manner to appropriate entities or, if appropriate, is made publicly available;

(2) an assessment of whether information has been appropriately classified and an accounting of the number of security clearances authorized by the Federal government for purposes of this title;

(3) a review of the type of cyber threat information shared with a cybersecurity center under section 102 of this Act, including whether such information meets the definition of cyber threat information under section 101, the degree to which such information may impact the privacy and civil liberties of individuals, any appropriate metrics to determine any impact of the sharing of such information with the Federal government on privacy and civil liberties, and the adequacy of any steps taken to reduce such impact;

(4) a review of actions taken by the Federal government based on information provided to a cybersecurity center under section 102 of this Act, including the appropriateness of any subsequent use under section 102(c)(1) of this Act and whether there was inappropriate stovepiping within the Federal government of any such information;

(5) a description of any violations of the requirements of this title by the Federal government;

(6) a classified list of entities that received classified information from the Federal government under section 103 of this Act and a description of any indication that such information may not have been appropriately handled;

(7) a summary of any breach of information security, if known, attributable to a specific failure by any entity or the Federal government to act on cyber threat information in the possession of such entity or the Federal government that resulted in substantial economic harm or injury to a specific entity or the Federal government; and

(8) any recommendation for improvements or modifications to the authorities under this title.

(b) FORM OF REPORT.—The report under subsection (a) shall be submitted in unclassified form, but shall include a classified annex.

SEC. 106. INSPECTOR GENERAL REVIEW.

(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency are authorized to review compliance by the cybersecurity centers, and by any Federal department or agency receiving cyber threat information from such cybersecurity centers, with the procedures required under section 102 of this Act.

(b) SCOPE OF REVIEW.—The review under subsection (a) shall consider whether the Federal government has handled such cyber threat information in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title.

(c) REPORT TO CONGRESS.—Each review conducted under this section shall be provided to Congress not later than 30 days after the date of completion of the review.

SEC. 107. TECHNICAL AMENDMENTS.

Section 552(b) of title 5, United States Code, is amended—

(1) in paragraph (8), by striking ''or'';

(2) in paragraph (9), by striking ''wells.'' and inserting ''wells; or''; and

(3) by adding at the end the following:

''(10) information shared with or provided to a cybersecurity center under section 102 of title I of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012.''.

SEC. 108. ACCESS TO CLASSIFIED INFORMATION.

(a) AUTHORIZATION REQUIRED.—No person shall be provided with access to classified information (as defined in section 6.1 of Executive Order 13526 (50 U.S.C. 435 note; relating to classified national security information)) relating to cyber security threats or cyber security vulnerabilities under this title without the appropriate security clearances.

(b) SECURITY CLEARANCES.—The appropriate Federal agencies or departments shall, consistent with applicable procedures and requirements, and if otherwise deemed appropriate, assist an individual in timely obtaining an appropriate security clearance where such individual has been determined to be eligible for such clearance and has a need-to-know (as defined in section 6.1 of that Executive Order) classified information to carry out this title.

TITLE II—COORDINATION OF FEDERAL INFORMATION SECURITY POLICY

SEC. 201. COORDINATION OF FEDERAL INFORMATION SECURITY POLICY.

(a) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by striking subchapters II and III and inserting the following:

''SUBCHAPTER II—INFORMATION SECURITY

''§ 3551. Purposes

''The purposes of this subchapter are—

''(1) to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

''(2) to recognize the highly networked nature of the current Federal computing environment and provide effective government-wide management of policies, directives, standards, and guidelines, as well as effective and nimble oversight of and response to information security risks, including coordination of information security efforts throughout the Federal civilian, national security, and law enforcement communities;

''(3) to provide for development and maintenance of controls required to protect agency information and information systems and contribute to the overall improvement of agency information security posture;

''(4) to provide for the development of tools and methods to assess and respond to real-time situational risk for Federal information system operations and assets; and

''(5) to provide a mechanism for improving agency information security programs through continuous monitoring of agency information systems and streamlined reporting requirements rather than overly prescriptive manual reporting.

''§ 3552. Definitions

''In this subchapter:

''(1) ADEQUATE SECURITY.—The term 'adequate security' means security commensurate with the risk and magnitude of the harm resulting from the unauthorized access to or loss, misuse, destruction, or modification of information.

''(2) AGENCY.—The term 'agency' has the meaning given the term in section 3502 of title 44.

''(3) CYBERSECURITY CENTER.—The term 'cybersecurity center' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

''(4) CYBER THREAT INFORMATION.—The term 'cyber threat information' means information that indicates or describes—

''(A) a technical or operation vulnerability or a cyber threat mitigation measure;

''(B) an action or operation to mitigate a cyber threat;

''(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

''(D) a method of defeating a technical control;

''(E) a method of defeating an operational control;

''(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

''(G) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to inadvertently enable the defeat of a technical or operational control;

''(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

''(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

''(J) any combination of subparagraphs (A) through (I).

''(5) DIRECTOR.—The term 'Director' means the Director of the Office of Management and Budget unless otherwise specified.

''(6) ENVIRONMENT OF OPERATION.—The term 'environment of operation' means the information system and environment in

which those systems operate, including changing threats, vulnerabilities, technologies, and missions and business practices.

''(7) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

''(8) INCIDENT.—The term 'incident' means an occurrence that—

''(A) actually or imminently jeopardizes the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores, or transmits; or

''(B) constitutes a violation of law or an imminent threat of violation of a law, a security policy, a security procedure, or an acceptable use policy.

''(9) INFORMATION RESOURCES.—The term 'information resources' has the meaning given the term in section 3502 of title 44.

''(10) INFORMATION SECURITY.—The term 'information security' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

''(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

''(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; or

''(C) availability, by ensuring timely and reliable access to and use of information.

''(11) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44.

''(12) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given the term in section 11101 of title 40.

''(13) MALICIOUS RECONNAISSANCE.—The term 'malicious reconnaissance' means a method for actively probing or passively monitoring an information system for the purpose of discerning technical vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

''(14) NATIONAL SECURITY SYSTEM.—

''(A) IN GENERAL.—The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

''(i) the function, operation, or use of which—

''(I) involves intelligence activities;

''(II) involves cryptologic activities related to national security;

''(III) involves command and control of military forces;

''(IV) involves equipment that is an integral part of a weapon or weapons system; or

''(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

''(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

''(B) LIMITATION.—Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

''(15) OPERATIONAL CONTROL.—The term 'operational control' means a security control for an information system that primarily is implemented and executed by people.

''(16) PERSON.—The term 'person' has the meaning given the term in section 3502 of title 44.

''(17) SECRETARY.—The term 'Secretary' means the Secretary of Commerce unless otherwise specified.

''(18) SECURITY CONTROL.—The term 'security control' means the management, operational, and technical controls, including safeguards or countermeasures, prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

''(19) SIGNIFICANT CYBER INCIDENT.—The term 'significant cyber incident' means a cyber incident resulting in, or an attempted cyber incident that, if successful, would have resulted in—

''(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

''(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

''(20) TECHNICAL CONTROL.—The term 'technical control' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

''§ 3553. Federal information security authority and coordination

''(a) IN GENERAL.—The Secretary, in consultation with the Secretary of Homeland Security, shall—

''(1) issue compulsory and binding policies and directives governing agency information security operations, and require implementation of such policies and directives, including—

''(A) policies and directives consistent with the standards and guidelines promulgated under section 11331 of title 40 to identify and provide information security protections prioritized and commensurate with the risk and impact resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by or on behalf of an agency; or

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(B) minimum operational requirements for Federal Government to protect agency information systems and provide common situational awareness across all agency information systems;

''(C) reporting requirements, consistent with relevant law, regarding information security incidents and cyber threat information;

''(D) requirements for agencywide information security programs;

''(E) performance requirements and metrics for the security of agency information systems;

''(F) training requirements to ensure that agencies are able to fully and timely comply with the policies and directives issued by the Secretary under this subchapter;

''(G) training requirements regarding privacy, civil rights, and civil liberties, and information oversight for agency information security personnel;

''(H) requirements for the annual reports to the Secretary under section 3554(d);

''(I) any other information security operations or information security requirements as determined by the Secretary in coordination with relevant agency heads; and

''(J) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

''(2) review the agencywide information security programs under section 3554; and

''(3) designate an individual or an entity at each cybersecurity center, among other responsibilities—

''(A) to receive reports and information about information security incidents, cyber threat information, and deterioration of security control affecting agency information systems; and

''(B) to act on or share the information under subparagraph (A) in accordance with this subchapter.

''(b) CONSIDERATIONS.—When issuing policies and directives under subsection (a), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology under section 11331 of title 40.

''(c) LIMITATION OF AUTHORITY.—The authorities of the Secretary under this section shall not apply to national security systems. Information security policies, directives, standards and guidelines for national security systems shall be overseen as directed by the President and, in accordance with that direction, carried out under the authority of the heads of agencies that operate or exercise authority over such national security systems.

''(d) STATUTORY CONSTRUCTION.—Nothing in this subchapter shall be construed to alter or amend any law regarding the authority of any head of an agency over such agency.

''§ 3554. Agency responsibilities

''(a) IN GENERAL.—The head of each agency shall—

''(1) be responsible for—

''(A) complying with the policies and directives issued under section 3553;

''(B) providing information security protections commensurate with the risk resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by the agency or by a contractor of an agency or other organization on behalf of an agency; and

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(C) complying with the requirements of this subchapter, including—

''(i) information security standards and guidelines promulgated under section 11331 of title 40;

''(ii) for any national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued as directed by the President; and

''(iii) for any non-national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued under section 3553;

''(D) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

''(E) reporting and sharing, for an agency operating or exercising control of a national security system, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated

at each cybersecurity center and to other appropriate entities consistent with policies and directives for national security systems issued as directed by the President; and

''(F) reporting and sharing, for those agencies operating or exercising control of non-national security systems, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for non-national security systems as prescribed under section 3553(a), including information to assist the entity designated under section 3555(a) with the ongoing security analysis under section 3555;

''(2) ensure that each senior agency official provides information security for the information and information systems that support the operations and assets under the senior agency official's control, including by—

''(A) assessing the risk and impact that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

''(B) determining the level of information security appropriate to protect such information and information systems in accordance with policies and directives issued under section 3553(a), and standards and guidelines promulgated under section 11331 of title 40 for information security classifications and related requirements;

''(C) implementing policies, procedures, and capabilities to reduce risks to an acceptable level in a cost-effective manner;

''(D) actively monitoring the effective implementation of information security controls and techniques; and

''(E) reporting information about information security incidents, cyber threat information, and deterioration of security controls in a timely and adequate manner to the entity designated under section 3553(a)(3) in accordance with paragraph (1);

''(3) assess and maintain the resiliency of information technology systems critical to agency mission and operations;

''(4) designate the agency Inspector General (or an independent entity selected in consultation with the Director and the Council of Inspectors General on Integrity and Efficiency if the agency does not have an Inspector General) to conduct the annual independent evaluation required under section 3556, and allow the agency Inspector General to contract with an independent entity to perform such evaluation;

''(5) delegate to the Chief Information Officer or equivalent (or to a senior agency official who reports to the Chief Information Officer or equivalent)—

''(A) the authority and primary responsibility to implement an agencywide information security program; and

''(B) the authority to provide information security for the information collected and maintained by the agency (or by a contractor, other agency, or other source on behalf of the agency) and for the information systems that support the operations, assets, and mission of the agency (including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency);

''(6) delegate to the appropriate agency official (who is responsible for a particular agency system or subsystem) the responsibility to ensure and enforce compliance with all requirements of the agency's agencywide information security program in coordination with the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5);

''(7) ensure that an agency has trained personnel who have obtained any necessary security clearances to permit them to assist the agency in complying with this subchapter;

''(8) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5), in coordination with other senior agency officials, reports to the agency head on the effectiveness of the agencywide information security program, including the progress of any remedial actions; and

''(9) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5) has the necessary qualifications to administer the functions described in this subchapter and has information security duties as a primary duty of that official.

''(b) CHIEF INFORMATION OFFICERS.—Each Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under subsection (a)(5) shall—

''(1) establish and maintain an enterprise security operations capability that on a continuous basis—

''(A) detects, reports, contains, mitigates, and responds to information security incidents that impair adequate security of the agency's information or information system in a timely manner and in accordance with the policies and directives under section 3553; and

''(B) reports any information security incident under subparagraph (A) to the entity designated under section 3555;

''(2) develop, maintain, and oversee an agencywide information security program;

''(3) develop, maintain, and oversee information security policies, procedures, and control techniques to address applicable requirements, including requirements under section 3553 of this title and section 11331 of title 40; and

''(4) train and oversee the agency personnel who have significant responsibility for information security with respect to that responsibility.

''(c) AGENCYWIDE INFORMATION SECURITY PROGRAMS.—

''(1) IN GENERAL.—Each agencywide information security program under subsection (b)(2) shall include—

''(A) relevant security risk assessments, including technical assessments and others related to the acquisition process;

''(B) security testing commensurate with risk and impact;

''(C) mitigation of deterioration of security controls commensurate with risk and impact;

''(D) risk-based continuous monitoring and threat assessment of the operational status and security of agency information systems to enable evaluation of the effectiveness of and compliance with information security policies, procedures, and practices, including a relevant and appropriate selection of security controls of information systems identified in the inventory under section 3505(c);

''(E) operation of appropriate technical capabilities in order to detect, mitigate, report, and respond to information security incidents, cyber threat information, and deterioration of security controls in a manner that is consistent with the policies and directives under section 3553, including—

''(i) mitigating risks associated with such information security incidents;

''(ii) notifying and consulting with the entity designated under section 3555; and

''(iii) notifying and consulting with, as appropriate—

''(I) law enforcement and the relevant Office of the Inspector General; and

''(II) any other entity, in accordance with law and as directed by the President;

''(F) a process to ensure that remedial action is taken to address any deficiencies in the information security policies, procedures, and practices of the agency; and

''(G) a plan and procedures to ensure the continuity of operations for information systems that support the operations and assets of the agency.

''(2) RISK MANAGEMENT STRATEGIES.—Each agencywide information security program under subsection (b)(2) shall include the development and maintenance of a risk management strategy for information security. The risk management strategy shall include—

''(A) consideration of information security incidents, cyber threat information, and deterioration of security controls; and

''(B) consideration of the consequences that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency;

''(3) POLICIES AND PROCEDURES.—Each agencywide information security program under subsection (b)(2) shall include policies and procedures that—

''(A) are based on the risk management strategy under paragraph (2);

''(B) reduce information security risks to an acceptable level in a cost-effective manner;

''(C) ensure that cost-effective and adequate information security is addressed as part of the acquisition and ongoing management of each agency information system; and

''(D) ensure compliance with—

''(i) this subchapter; and

''(ii) any other applicable requirements.

''(4) TRAINING REQUIREMENTS.—Each agencywide information security program under subsection (b)(2) shall include information security, privacy, civil rights, civil liberties, and information oversight training that meets any applicable requirements under section 3553. The training shall inform each information security personnel that has access to agency information systems (including contractors and other users of information systems that support the operations and assets of the agency) of—

''(A) the information security risks associated with the information security personnel's activities; and

''(B) the individual's responsibility to comply with the agency policies and procedures that reduce the risks under subparagraph (A).

''(d) ANNUAL REPORT.—Each agency shall submit a report annually to the Secretary of Homeland Security on its agencywide information security program and information systems.

''§ 3555. Multiagency ongoing threat assessment

''(a) IMPLEMENTATION.—The Director of the Office of Management and Budget, in coordination with the Secretary of Homeland Security, shall designate an entity to implement ongoing security analysis concerning agency information systems—

''(1) based on cyber threat information;

''(2) based on agency information system and environment of operation changes, including—

''(A) an ongoing evaluation of the information system security controls; and

''(B) the security state, risk level, and environment of operation of an agency information system, including—

''(i) a change in risk level due to a new cyber threat;

''(ii) a change resulting from a new technology;

''(iii) a change resulting from the agency's mission; and

''(iv) a change resulting from the business practice; and

''(3) using automated processes to the maximum extent possible—

''(A) to increase information system security;

''(B) to reduce paper-based reporting requirements; and

''(C) to maintain timely and actionable knowledge of the state of the information system security.

''(b) STANDARDS.—The National Institute of Standards and Technology may promulgate standards, in coordination with the Secretary of Homeland Security, to assist an agency with its duties under this section.

''(c) COMPLIANCE.—The head of each appropriate department and agency shall be responsible for ensuring compliance and implementing necessary procedures to comply with this section. The head of each appropriate department and agency, in consultation with the Director of the Office of Management and Budget and the Secretary of Homeland Security, shall—

''(1) monitor compliance under this section;

''(2) develop a timeline and implement for the department or agency—

''(A) adoption of any technology, system, or method that facilitates continuous monitoring and threat assessments of an agency information system;

''(B) adoption or updating of any technology, system, or method that prevents, detects, or remediates a significant cyber incident to a Federal information system of the department or agency that has impeded, or is reasonably likely to impede, the performance of a critical mission of the department or agency; and

''(C) adoption of any technology, system, or method that satisfies a requirement under this section.

''(d) LIMITATION OF AUTHORITY.—The authorities of the Director of the Office of Management and Budget and of the Secretary of Homeland Security under this section shall not apply to national security systems.

''(e) REPORT.—Not later than 6 months after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Government Accountability Office shall issue a report evaluating each agency's status toward implementing this section.

''§ 3556. Independent evaluations

''(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency, in consultation with the Director and the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense, shall issue and maintain criteria for the timely, cost-effective, risk-based, and independent evaluation of each agencywide information security program (and practices) to determine the effectiveness of the agencywide information security program (and practices). The criteria shall include measures to assess any conflicts of interest in the performance of the evaluation and whether the agencywide information security program includes appropriate safeguards against disclosure of information where such disclosure may adversely affect information security.

''(b) ANNUAL INDEPENDENT EVALUATIONS.—Each agency shall perform an annual independent evaluation of its agencywide information security program (and practices) in accordance with the criteria under subsection (a).

''(c) DISTRIBUTION OF REPORTS.—Not later than 30 days after receiving an independent evaluation under subsection (b), each agency head shall transmit a copy of the independent evaluation to the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense.

''(d) NATIONAL SECURITY SYSTEMS.—Evaluations involving national security systems shall be conducted as directed by President.

''§ 3557. National security systems.

''The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

''(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system; and

''(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President.''.

(b) SAVINGS PROVISIONS.—

(1) POLICY AND COMPLIANCE GUIDANCE.—Policy and compliance guidance issued by the Director before the date of enactment of this Act under section 3543(a)(1) of title 44, United States Code (as in effect on the day before the date of enactment of this Act), shall continue in effect, according to its terms, until modified, terminated, superseded, or repealed pursuant to section 3553(a)(1) of title 44, United States Code.

(2) STANDARDS AND GUIDELINES.—Standards and guidelines issued by the Secretary of Commerce or by the Director before the date of enactment of this Act under section 11331(a)(1) of title 40, United States Code, (as in effect on the day before the date of enactment of this Act) shall continue in effect, according to their terms, until modified, terminated, superseded, or repealed pursuant to section 11331(a)(1) of title 40, United States Code, as amended by this Act.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) CHAPTER ANALYSIS.—The chapter analysis for chapter 35 of title 44, United States Code, is amended—

(A) by striking the items relating to sections 3531 through 3538;

(B) by striking the items relating to sections 3541 through 3549; and

(C) by inserting the following:

''3551. Purposes.
''3552. Definitions.
''3553. Federal information security authority and coordination.
''3554. Agency responsibilities.
''3555. Multiagency ongoing threat assessment.
''3556. Independent evaluations.
''3557. National security systems.''.

(2) OTHER REFERENCES.—

(A) Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(1)(A)) is amended by striking ''section 3532(3)'' and inserting ''section 3552''.

(B) Section 2222(j)(5) of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(C) Section 2223(c)(3) of title 10, United States Code, is amended, by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(D) Section 2315 of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(E) Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended—

(i) in subsection (a)(2), by striking ''section 3532(b)(2)'' and inserting ''section 3552'';

(ii) in subsection (c)(3), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iii) in subsection (d)(1), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iv) in subsection (d)(8) by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(v) in subsection (d)(8), by striking ''submitted to the Director'' and inserting ''submitted to the Secretary'';

(vi) in subsection (e)(2), by striking ''section 3532(1) of such title'' and inserting ''section 3552 of title 44''; and

(vii) in subsection (e)(5), by striking ''section 3532(b)(2) of such title'' and inserting ''section 3552 of title 44''.

(F) Section 8(d)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7406(d)(1)) is amended by striking ''section 3534(b)'' and inserting ''section 3554(b)(2)''.

SEC. 202. MANAGEMENT OF INFORMATION TECHNOLOGY.

(a) IN GENERAL.—Section 11331 of title 40, United States Code, is amended to read as follows:

''§ 11331. Responsibilities for Federal information systems standards

''(a) STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO PRESCRIBE.—Except as provided under paragraph (2), the Secretary of Commerce shall prescribe standards and guidelines pertaining to Federal information systems—

''(A) in consultation with the Secretary of Homeland Security; and

''(B) on the basis of standards and guidelines developed by the National Institute of Standards and Technology under paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)(2) and (a)(3)).

''(2) NATIONAL SECURITY SYSTEMS.—Standards and guidelines for national security systems shall be developed, prescribed, enforced, and overseen as otherwise authorized by law and as directed by the President.

''(b) MANDATORY STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO MAKE MANDATORY STANDARDS AND GUIDELINES.—The Secretary of Commerce shall make standards and guidelines under subsection (a)(1) compulsory and binding to the extent determined necessary by the Secretary of Commerce to improve the efficiency of operation or security of Federal information systems.

''(2) REQUIRED MANDATORY STANDARDS AND GUIDELINES.—

''(A) IN GENERAL.—Standards and guidelines under subsection (a)(1) shall include information security standards that—

''(i) provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)); and

''(ii) are otherwise necessary to improve the security of Federal information and information systems.

''(B) BINDING EFFECT.—Information security standards under subparagraph (A) shall be compulsory and binding.

''(c) EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary of Commerce shall exercise the authority conferred by this section subject to direction by the President and in coordination with the Director.

''(d) APPLICATION OF MORE STRINGENT STANDARDS AND GUIDELINES.—The head of an executive agency may employ standards for the cost-effective information security for

information systems within or under the supervision of that agency that are more stringent than the standards and guidelines the Secretary of Commerce prescribes under this section if the more stringent standards and guidelines—

''(1) contain at least the applicable standards and guidelines made compulsory and binding by the Secretary of Commerce; and

''(2) are otherwise consistent with the policies, directives, and implementation memoranda issued under section 3553(a) of title 44.

''(e) DECISIONS ON PROMULGATION OF STANDARDS AND GUIDELINES.—The decision by the Secretary of Commerce regarding the promulgation of any standard or guideline under this section shall occur not later than 6 months after the date of submission of the proposed standard to the Secretary of Commerce by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

''(f) NOTICE AND COMMENT.—A decision by the Secretary of Commerce to significantly modify, or not promulgate, a proposed standard submitted to the Secretary by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) shall be made after the public is given an opportunity to comment on the Secretary's proposed decision.

''(g) DEFINITIONS.—In this section:

''(1) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' has the meaning given the term in section 3552 of title 44.

''(2) INFORMATION SECURITY.—The term 'information security' has the meaning given the term in section 3552 of title 44.

''(3) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given the term in section 3552 of title 44.''.

SEC. 203. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 204. TECHNICAL AND CONFORMING AMENDMENTS.

Section 21(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4(b)) is amended—

(1) in paragraph (2), by striking ''and the Director of the Office of Management and Budget'' and inserting '', the Secretary of Commerce, and the Secretary of Homeland Security''; and

(2) in paragraph (3), by inserting '', the Secretary of Homeland Security,'' after ''the Secretary of Commerce''.

SEC. 205. CLARIFICATION OF AUTHORITIES.

Nothing in this title shall be construed to convey any new regulatory authority to any government entity implementing or complying with any provision of this title.

TITLE III—CRIMINAL PENALTIES

SEC. 301. PENALTIES FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030(c) of title 18, United States Code, is amended to read as follows:

''(c) The punishment for an offense under subsection (a) or (b) of this section is—

''(1) a fine under this title or imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(1) of this section;

''(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than 3 years, or both, in the case of an offense under subsection (a)(2); or

''(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2) of this section, if—

''(i) the offense was committed for purposes of commercial advantage or private financial gain;

''(ii) the offense was committed in the furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States, or of any State; or

''(iii) the value of the information obtained, or that would have been obtained if the offense was completed, exceeds $5,000;

''(3) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(3) of this section;

''(4) a fine under this title or imprisonment of not more than 20 years, or both, in the case of an offense under subsection (a)(4) of this section;

''(5)(A) except as provided in subparagraph (C), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A) of this section, if the offense caused—

''(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

''(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

''(iii) physical injury to any person;

''(iv) a threat to public health or safety;

''(v) damage affecting a computer used by, or on behalf of, an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

''(vi) damage affecting 10 or more protected computers during any 1-year period;

''(B) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(B), if the offense caused a harm provided in clause (i) through (vi) of subparagraph (A) of this subsection;

''(C) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both;

''(D) a fine under this title, imprisonment for not more than 10 years, or both, for any other offense under subsection (a)(5);

''(E) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(6) of this section; or

''(F) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(7) of this section.''.

SEC. 302. TRAFFICKING IN PASSWORDS.

Section 1030(a)(6) of title 18, United States Code, is amended to read as follows:

''(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information or means of access through which a protected computer (as defined in subparagraphs (A) and (B) of subsection (e)(2)) may be accessed without authorization.''.

SEC. 303. CONSPIRACY AND ATTEMPTED COMPUTER FRAUD OFFENSES.

Section 1030(b) of title 18, United States Code, is amended by inserting ''as if for the completed offense'' after ''punished as provided''.

SEC. 304. CRIMINAL AND CIVIL FORFEITURE FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030 of title 18, United States Code, is amended by striking subsections (i) and (j) and inserting the following:

''(i) CRIMINAL FORFEITURE.—

''(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

''(A) such person's interest in any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of such violation; and

''(B) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of such violation.

''(2) The criminal forfeiture of property under this subsection, including any seizure and disposition of the property, and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

''(j) CIVIL FORFEITURE.—

''(1) The following shall be subject to forfeiture to the United States and no property right, real or personal, shall exist in them:

''(A) Any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of any violation of this section, or a conspiracy to violate this section.

''(B) Any property, real or personal, constituting or derived from any gross proceeds obtained directly or indirectly, or any property traceable to such property, as a result of the commission of any violation of this section, or a conspiracy to violate this section.

''(2) Seizures and forfeitures under this subsection shall be governed by the provisions in chapter 46 relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents and other persons as may be designated for that purpose by the Secretary of Homeland Security or the Attorney General.''.

SEC. 305. DAMAGE TO CRITICAL INFRASTRUCTURE COMPUTERS.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

''§ 1030A. Aggravated damage to a critical infrastructure computer

''(a) DEFINITIONS.—In this section—

''(1) the term 'computer' has the meaning given the term in section 1030;

''(2) the term 'critical infrastructure computer' means a computer that manages or controls systems or assets vital to national defense, national security, national economic security, public health or safety, or any combination of those matters, whether publicly or privately owned or operated, including—

''(A) oil and gas production, storage, conversion, and delivery systems;

''(B) water supply systems;

''(C) telecommunication networks;

''(D) electrical power generation and delivery systems;

''(E) finance and banking systems;

''(F) emergency services;

''(G) transportation systems and services; and

''(H) government operations that provide essential services to the public; and

''(3) the term 'damage' has the meaning given the term in section 1030.

''(b) OFFENSE.—It shall be unlawful, during and in relation to a felony violation of section 1030, to knowingly cause or attempt to cause damage to a critical infrastructure computer if the damage results in (or, in the

case of an attempt, if completed, would have resulted in) the substantial impairment—

''(1) of the operation of the critical infrastructure computer; or

''(2) of the critical infrastructure associated with the computer.

''(c) PENALTY.—Any person who violates subsection (b) shall be—

''(1) fined under this title;

''(2) imprisoned for not less than 3 years but not more than 20 years; or

''(3) penalized under paragraphs (1) and (2).

''(d) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

''(1) a court shall not place on probation any person convicted of a violation of this section;

''(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment, including any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for a felony violation of section 1030;

''(3) in determining any term of imprisonment to be imposed for a felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The chapter analysis for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

''1030A. Aggravated damage to a critical infrastructure computer.''.

SEC. 306. LIMITATION ON ACTIONS INVOLVING UNAUTHORIZED USE.

Section 1030(e)(6) of title 18, United States Code, is amended by striking ''alter;'' and inserting ''alter, but does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized;''.

SEC. 307. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

TITLE IV—CYBERSECURITY RESEARCH AND DEVELOPMENT

SEC. 401. NATIONAL HIGH-PERFORMANCE COMPUTING PROGRAM PLANNING AND COORDINATION.

(a) GOALS AND PRIORITIES.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(d) GOALS AND PRIORITIES.—The goals and priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include—

''(1) encouraging and supporting mechanisms for interdisciplinary research and development in networking and information technology, including—

''(A) through collaborations across agencies;

''(B) through collaborations across Program Component Areas;

''(C) through collaborations with industry;

''(D) through collaborations with institutions of higher education;

''(E) through collaborations with Federal laboratories (as defined in section 4 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3703)); and

''(F) through collaborations with international organizations;

''(2) addressing national, multi-agency, multi-faceted challenges of national importance; and

''(3) fostering the transfer of research and development results into new technologies and applications for the benefit of society.''.

(b) DEVELOPMENT OF STRATEGIC PLAN.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(e) STRATEGIC PLAN.—

''(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the agencies under subsection (a)(3)(B), working through the National Science and Technology Council and with the assistance of the Office of Science and Technology Policy shall develop a 5-year strategic plan to guide the activities under subsection (a)(1).

''(2) CONTENTS.—The strategic plan shall specify—

''(A) the near-term objectives for the Program;

''(B) the long-term objectives for the Program;

''(C) the anticipated time frame for achieving the near-term objectives;

''(D) the metrics that will be used to assess any progress made toward achieving the near-term objectives and the long-term objectives; and

''(E) how the Program will achieve the goals and priorities under subsection (d).

''(3) IMPLEMENTATION ROADMAP.—

''(A) IN GENERAL.—The agencies under subsection (a)(3)(B) shall develop and annually update an implementation roadmap for the strategic plan.

''(B) REQUIREMENTS.—The information in the implementation roadmap shall be coordinated with the database under section 102(c) and the annual report under section 101(a)(3). The implementation roadmap shall—

''(i) specify the role of each Federal agency in carrying out or sponsoring research and development to meet the research objectives of the strategic plan, including a description of how progress toward the research objectives will be evaluated, with consideration of any relevant recommendations of the advisory committee;

''(ii) specify the funding allocated to each major research objective of the strategic plan and the source of funding by agency for the current fiscal year; and

''(iii) estimate the funding required for each major research objective of the strategic plan for the next 3 fiscal years.

''(4) RECOMMENDATIONS.—The agencies under subsection (a)(3)(B) shall take into consideration when developing the strategic plan under paragraph (1) the recommendations of—

''(A) the advisory committee under subsection (b); and

''(B) the stakeholders under section 102(a)(3).

''(5) REPORT TO CONGRESS.—The Director of the Office of Science and Technology Policy shall transmit the strategic plan under this subsection, including the implementation roadmap and any updates under paragraph (3), to—

''(A) the advisory committee under subsection (b);

''(B) the Committee on Commerce, Science, and Transportation of the Senate; and

''(C) the Committee on Science and Technology of the House of Representatives.''.

(c) PERIODIC REVIEWS.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(f) PERIODIC REVIEWS.—The agencies under subsection (a)(3)(B) shall—

''(1) periodically assess the contents and funding levels of the Program Component Areas and restructure the Program when warranted, taking into consideration any relevant recommendations of the advisory committee under subsection (b); and

''(2) ensure that the Program includes national, multi-agency, multi-faceted research and development activities, including activities described in section 104.''.

(d) ADDITIONAL RESPONSIBILITIES OF DIRECTOR.—Section 101(a)(2) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(2)) is amended—

(1) by redesignating subparagraphs (E) and (F) as subparagraphs (G) and (H), respectively; and

(2) by inserting after subparagraph (D) the following:

''(E) encourage and monitor the efforts of the agencies participating in the Program to allocate the level of resources and management attention necessary—

''(i) to ensure that the strategic plan under subsection (e) is developed and executed effectively; and

''(ii) to ensure that the objectives of the Program are met;

''(F) working with the Office of Management and Budget and in coordination with the creation of the database under section 102(c), direct the Office of Science and Technology Policy and the agencies participating in the Program to establish a mechanism (consistent with existing law) to track all ongoing and completed research and development projects and associated funding;''.

(e) ADVISORY COMMITTEE.—Section 101(b) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(b)) is amended—

(1) in paragraph (1)—

(A) by inserting after the first sentence the following: ''The co-chairs of the advisory committee shall meet the qualifications of committee members and may be members of the Presidents Council of Advisors on Science and Technology.''; and

(B) by striking ''high-performance'' in subparagraph (D) and inserting ''high-end''; and

(2) by amending paragraph (2) to read as follows:

''(2) In addition to the duties under paragraph (1), the advisory committee shall conduct periodic evaluations of the funding, management, coordination, implementation, and activities of the Program. The advisory committee shall report its findings and recommendations not less frequently than once every 3 fiscal years to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives. The report shall be submitted in conjunction with the update of the strategic plan.''.

(f) REPORT.—Section 101(a)(3) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(3)) is amended—

(1) in subparagraph (C)—

(A) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(B) by striking ''each Program Component Area'' and inserting ''each Program Component Area and each research area supported in accordance with section 104'';

(2) in subparagraph (D)—

(A) by striking ''each Program Component Area,'' and inserting ''each Program Component Area and each research area supported in accordance with section 104,'';

(B) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(C) by striking ''and'' after the semicolon;

(3) by redesignating subparagraph (E) as subparagraph (G); and

(4) by inserting after subparagraph (D) the following:

''(E) include a description of how the objectives for each Program Component Area, and the objectives for activities that involve multiple Program Component Areas, relate to the objectives of the Program identified in the strategic plan under subsection (e);

''(F) include—

''(i) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the next fiscal year by category of activity;

''(ii) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the current fiscal year by category of activity; and

''(iii) the amount of funding provided for the Office of Science and Technology Policy for the current fiscal year by each agency participating in the Program; and''.

(g) DEFINITIONS.—Section 4 of the High-Performance Computing Act of 1991 (15 U.S.C. 5503) is amended—

(1) by redesignating paragraphs (1) and (2) as paragraphs (2) and (3), respectively;

(2) by redesignating paragraph (3) as paragraph (6);

(3) by redesignating paragraphs (6) and (7) as paragraphs (7) and (8), respectively;

(4) by inserting before paragraph (2), as redesignated, the following:

''(1) 'cyber-physical systems' means physical or engineered systems whose networking and information technology functions and physical elements are deeply integrated and are actively connected to the physical world through sensors, actuators, or other means to perform monitoring and control functions;'';

(5) in paragraph (3), as redesignated, by striking ''high-performance computing'' and inserting ''networking and information technology'';

(6) in paragraph (6), as redesignated—

(A) by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(B) by striking ''supercomputer'' and inserting ''high-end computing'';

(7) in paragraph (5), by striking ''network referred to as'' and all that follows through the semicolon and inserting ''network, including advanced computer networks of Federal agencies and departments''; and

(8) in paragraph (7), as redesignated, by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program''.

SEC. 402. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

(a) RESEARCH IN AREAS OF NATIONAL IMPORTANCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.) is amended by adding at the end the following:

''SEC. 104. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

''(a) IN GENERAL.—The Program shall encourage agencies under section 101(a)(3)(B) to support, maintain, and improve national, multi-agency, multi-faceted, research and development activities in networking and information technology directed toward application areas that have the potential for significant contributions to national economic competitiveness and for other significant societal benefits.

''(b) TECHNICAL SOLUTIONS.—An activity under subsection (a) shall be designed to advance the development of research discoveries by demonstrating technical solutions to important problems in areas including—

''(1) cybersecurity;

''(2) health care;

''(3) energy management and low-power systems and devices;

''(4) transportation, including surface and air transportation;

''(5) cyber-physical systems;

''(6) large-scale data analysis and modeling of physical phenomena;

''(7) large scale data analysis and modeling of behavioral phenomena;

''(8) supply chain quality and security; and

''(9) privacy protection and protected disclosure of confidential data.

''(c) RECOMMENDATIONS.—The advisory committee under section 101(b) shall make recommendations to the Program for candidate research and development areas for support under this section.

''(d) CHARACTERISTICS.—

''(1) IN GENERAL.—Research and development activities under this section—

''(A) shall include projects selected on the basis of applications for support through a competitive, merit-based process;

''(B) shall leverage, when possible, Federal investments through collaboration with related State initiatives;

''(C) shall include a plan for fostering the transfer of research discoveries and the results of technology demonstration activities, including from institutions of higher education and Federal laboratories, to industry for commercial development;

''(D) shall involve collaborations among researchers in institutions of higher education and industry; and

''(E) may involve collaborations among nonprofit research institutions and Federal laboratories, as appropriate.

''(2) COST-SHARING.—In selecting applications for support, the agencies under section 101(a)(3)(B) shall give special consideration to projects that include cost sharing from non-Federal sources.

''(3) MULTIDISCIPLINARY RESEARCH CENTERS.—Research and development activities under this section shall be supported through multidisciplinary research centers, including Federal laboratories, that are organized to investigate basic research questions and carry out technology demonstration activities in areas described in subsection (a). Research may be carried out through existing multidisciplinary centers, including those authorized under section 7024(b)(2) of the America COMPETES Act (42 U.S.C. 1862o–10(2)).''.

(b) CYBER-PHYSICAL SYSTEMS.—Section 101(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following:

''(J) provide for increased understanding of the scientific principles of cyber-physical systems and improve the methods available for the design, development, and operation of cyber-physical systems that are characterized by high reliability, safety, and security; and

''(K) provide for research and development on human-computer interactions, visualization, and big data.''.

(c) TASK FORCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.), as amended by section 402(a) of this Act, is amended by adding at the end the following:

''SEC. 105. TASK FORCE.

''(a) ESTABLISHMENT.—Not later than 180 days after the date of enactment the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy under section 102 shall convene a task force to explore mechanisms for carrying out collaborative research and development activities for cyber-physical systems (including the related technologies required to enable these systems) through a consortium or other appropriate entity with participants from institutions of higher education, Federal laboratories, and industry.

''(b) FUNCTIONS.—The task force shall—

''(1) develop options for a collaborative model and an organizational structure for such entity under which the joint research and development activities could be planned, managed, and conducted effectively, including mechanisms for the allocation of resources among the participants in such entity for support of such activities;

''(2) propose a process for developing a research and development agenda for such entity, including guidelines to ensure an appropriate scope of work focused on nationally significant challenges and requiring collaboration and to ensure the development of related scientific and technological milestones;

''(3) define the roles and responsibilities for the participants from institutions of higher education, Federal laboratories, and industry in such entity;

''(4) propose guidelines for assigning intellectual property rights and for transferring research results to the private sector; and

''(5) make recommendations for how such entity could be funded from Federal, State, and non-governmental sources.

''(c) COMPOSITION.—In establishing the task force under subsection (a), the Director of the Office of Science and Technology Policy shall appoint an equal number of individuals from institutions of higher education and from industry with knowledge and expertise in cyber-physical systems, and may appoint not more than 2 individuals from Federal laboratories.

''(d) REPORT.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy shall transmit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives a report describing the findings and recommendations of the task force.

''(e) TERMINATION.—The task force shall terminate upon transmittal of the report required under subsection (d).

''(f) COMPENSATION AND EXPENSES.—Members of the task force shall serve without compensation.''.

SEC. 403. PROGRAM IMPROVEMENTS.

Section 102 of the High-Performance Computing Act of 1991 (15 U.S.C. 5512) is amended to read as follows:

''SEC. 102. PROGRAM IMPROVEMENTS.

''(a) FUNCTIONS.—The Director of the Office of Science and Technology Policy shall continue—

''(1) to provide technical and administrative support to—

''(A) the agencies participating in planning and implementing the Program, including support needed to develop the strategic plan under section 101(e); and

''(B) the advisory committee under section 101(b);

SA 2606. Mr. MCCAIN (for himself, Mrs. HUTCHISON, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 1, strike line 3 and all that follows through page 211, line 6 and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012'' or ''SECURE IT''.

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

TITLE I—FACILITATING SHARING OF CYBER THREAT INFORMATION

SEC. 101. DEFINITIONS.

In this title:

(1) AGENCY.—The term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code.

(2) ANTITRUST LAWS.—The term ''antitrust laws''—

(A) has the meaning given the term in section 1(a) of the Clayton Act (15 U.S.C. 12(a));

(B) includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that section 5 of that Act applies to unfair methods of competition; and

(C) includes any State law that has the same intent and effect as the laws under subparagraphs (A) and (B).

(3) COUNTERMEASURE.—The term ''countermeasure'' means an automated or a manual action with defensive intent to mitigate cyber threats.

(4) CYBER THREAT INFORMATION.—The term ''cyber threat information'' means information that indicates or describes—

(A) a technical or operation vulnerability or a cyber threat mitigation measure;

(B) an action or operation to mitigate a cyber threat;

(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

(D) a method of defeating a technical control;

(E) a method of defeating an operational control;

(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

(G) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to inadvertently enable the defeat of a technical or operational control;

(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

(J) any combination of subparagraphs (A) through (I).

(5) CYBERSECURITY CENTER.—The term ''cybersecurity center'' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

(6) CYBERSECURITY SYSTEM.—The term ''cybersecurity system'' means a system designed or employed to ensure the integrity, confidentiality, or availability of, or to safeguard, a system or network, including measures intended to protect a system or network from—

(A) efforts to degrade, disrupt, or destroy such system or network; or

(B) theft or misappropriations of private or government information, intellectual property, or personally identifiable information.

(7) ENTITY.—

(A) IN GENERAL.—The term ''entity'' means any private entity, non-Federal government agency or department, or State, tribal, or local government agency or department (including an officer, employee, or agent thereof).

(B) INCLUSIONS.—The term ''entity'' includes a government agency or department (including an officer, employee, or agent thereof) of the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States.

(8) FEDERAL INFORMATION SYSTEM.—The term ''Federal information system'' means an information system of a Federal department or agency used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

(9) INFORMATION SECURITY.—The term ''information security'' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; or

(C) availability, by ensuring timely and reliable access to and use of information.

(10) INFORMATION SYSTEM.—The term ''information system'' has the meaning given the term in section 3502 of title 44, United States Code.

(11) LOCAL GOVERNMENT.—The term ''local government'' means any borough, city, county, parish, town, township, village, or other general purpose political subdivision of a State.

(12) MALICIOUS RECONNAISSANCE.—The term ''malicious reconnaissance'' means a method for actively probing or passively monitoring an information system for the purpose of discerning technical vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(13) OPERATIONAL CONTROL.—The term ''operational control'' means a security control for an information system that primarily is implemented and executed by people.

(14) OPERATIONAL VULNERABILITY.—The term ''operational vulnerability'' means any attribute of policy, process, or procedure that could enable or facilitate the defeat of an operational control.

(15) PRIVATE ENTITY.—The term ''private entity'' means any individual or any private group, organization, or corporation, including an officer, employee, or agent thereof.

(16) SIGNIFICANT CYBER INCIDENT.—The term ''significant cyber incident'' means a cyber incident resulting in, or an attempted cyber incident that, if successful, would have resulted in—

(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

(17) TECHNICAL CONTROL.—The term ''technical control'' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

(18) TECHNICAL VULNERABILITY.—The term ''technical vulnerability'' means any attribute of hardware or software that could enable or facilitate the defeat of a technical control.

(19) TRIBAL.—The term ''tribal'' has the meaning given the term ''Indian tribe'' in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

SEC. 102. AUTHORIZATION TO SHARE CYBER THREAT INFORMATION.

(a) VOLUNTARY DISCLOSURE.—

(1) PRIVATE ENTITIES.—Notwithstanding any other provision of law, a private entity may, for the purpose of preventing, investigating, or otherwise mitigating threats to information security, on its own networks, or as authorized by another entity, on such entity's networks, employ countermeasures and use cybersecurity systems in order to obtain, identify, or otherwise possess cyber threat information.

(2) ENTITIES.—Notwithstanding any other provision of law, an entity may disclose cyber threat information to—

(A) a cybersecurity center; or

(B) any other entity in order to assist with preventing, investigating, or otherwise mitigating threats to information security.

(3) INFORMATION SECURITY PROVIDERS.—If the cyber threat information described in paragraph (1) is obtained, identified, or otherwise possessed in the course of providing information security products or services under contract to another entity, that entity shall be given, at any time prior to disclosure of such information, a reasonable opportunity to authorize or prevent such disclosure, to request anonymization of such information, or to request that reasonable efforts be made to safeguard such information that identifies specific persons from unauthorized access or disclosure.

(b) SIGNIFICANT CYBER INCIDENTS INVOLVING FEDERAL INFORMATION SYSTEMS.—

(1) IN GENERAL.—An entity providing electronic communication services, remote computing services, or information security services to a Federal department or agency shall inform the Federal department or agency of a significant cyber incident involving the Federal information system of that Federal department or agency that—

(A) is directly known to the entity as a result of providing such services;

(B) is directly related to the provision of such services by the entity; and

(C) as determined by the entity, has impeded or will impede the performance of a critical mission of the Federal department or agency.

(2) ADVANCE COORDINATION.—A Federal department or agency receiving the services described in paragraph (1) shall coordinate in advance with an entity described in paragraph (1) to develop the parameters of any information that may be provided under paragraph (1), including clarification of the type of significant cyber incident that will impede the performance of a critical mission of the Federal department or agency.

(3) REPORT.—A Federal department or agency shall report information provided under this subsection to a cybersecurity center.

(4) CONSTRUCTION.—Any information provided to a cybersecurity center under paragraph (3) shall be treated in the same manner as information provided to a cybersecurity center under subsection (a).

(c) INFORMATION SHARED WITH OR PROVIDED TO A CYBERSECURITY CENTER.—Cyber threat information provided to a cybersecurity center under this section—

(1) may be disclosed to, retained by, and used by, consistent with otherwise applicable Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal government for a cybersecurity purpose, a national security purpose, or in order to prevent, investigate, or prosecute any of the offenses listed in section 2516 of title 18, United States Code, and such information shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under this paragraph;

(2) may, with the prior written consent of the entity submitting such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(3) shall be considered the commercial, financial, or proprietary information of the entity providing such information to the Federal government and any disclosure outside the Federal government may only be made upon the prior written consent by such entity and shall not constitute a waiver of any applicable privilege or protection provided by law, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(4) shall be deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records;

(5) shall be, without discretion, withheld from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records;

(6) shall not be subject to the rules of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official;

(7) shall not, if subsequently provided to a State, tribal, or local government or government agency, otherwise be disclosed or distributed to any entity by such State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent; and

(8) shall not be directly used by any Federal, State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph.

(d) PROCEDURES RELATING TO INFORMATION SHARING WITH A CYBERSECURITY CENTER.—Not later than 60 days after the date of enactment of this Act, the heads of each department or agency containing a cybersecurity center shall jointly develop, promulgate, and submit to Congress procedures to ensure that cyber threat information shared with or provided to—

(1) a cybersecurity center under this section—

(A) may be submitted to a cybersecurity center by an entity, to the greatest extent possible, through a uniform, publicly available process or format that is easily accessible on the website of such cybersecurity center, and that includes the ability to provide relevant details about the cyber threat information and written consent to any subsequent disclosures authorized by this paragraph;

(B) shall immediately be further shared with each cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government;

(C) is handled by the Federal government in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title, and the Federal government may undertake efforts consistent with this subparagraph to limit the impact on privacy and civil liberties of the sharing of cyber threat information with the Federal government; and

(D) except as provided in this section, shall only be used, disclosed, or handled in accordance with the provisions of subsection (c); and

(2) a Federal agency or department under subsection (b) is provided immediately to a cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government.

(e) INFORMATION SHARED BETWEEN ENTITIES.—

(1) IN GENERAL.—An entity sharing cyber threat information with another entity under this title may restrict the use or sharing of such information by such other entity.

(2) FURTHER SHARING.—Cyber threat information shared by any entity with another entity under this title—

(A) shall only be further shared in accordance with any restrictions placed on the sharing of such information by the entity authorizing such sharing, such as appropriate anonymization of such information; and

(B) may not be used by any entity to gain an unfair competitive advantage to the detriment of the entity authorizing the sharing of such information, except that the conduct described in paragraph (3) shall not constitute unfair competitive conduct.

(3) INFORMATION SHARED WITH STATE, TRIBAL, OR LOCAL GOVERNMENT OR GOVERNMENT AGENCY.—Cyber threat information shared with a State, tribal, or local government or government agency under this title—

(A) may, with the prior written consent of the entity sharing such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent;

(B) shall be deemed voluntarily shared information and exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records;

(C) shall not be disclosed or distributed to any entity by the State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any

State, tribal, or local law requiring disclosure of information or records, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent; and

(D) shall not be directly used by any State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this subparagraph.

(4) ANTITRUST EXEMPTION.—The exchange or provision of cyber threat information or assistance between 2 or more private entities under this title shall not be considered a violation of any provision of antitrust laws if exchanged or provided in order to assist with—

(A) facilitating the prevention, investigation, or mitigation of threats to information security; or

(B) communicating or disclosing of cyber threat information to help prevent, investigate or otherwise mitigate the effects of a threat to information security.

(5) NO RIGHT OR BENEFIT.—The provision of cyber threat information to an entity under this section shall not create a right or a benefit to similar information by such entity or any other entity.

(f) FEDERAL PREEMPTION.—

(1) IN GENERAL.—This section supersedes any statute or other law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this section.

(2) STATE LAW ENFORCEMENT.—Nothing in this section shall be construed to supersede any statute or other law of a State or political subdivision of a State concerning the use of authorized law enforcement techniques.

(3) PUBLIC DISCLOSURE.—No information shared with or provided to a State, tribal, or local government or government agency pursuant to this section shall be made publicly available pursuant to any State, tribal, or local law requiring disclosure of information or records.

(g) CIVIL AND CRIMINAL LIABILITY.—

(1) GENERAL PROTECTIONS.—

(A) PRIVATE ENTITIES.—No cause of action shall lie or be maintained in any court against any private entity for—

(i) the use of countermeasures and cybersecurity systems as authorized by this title;

(ii) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(iii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such private entity.

(B) ENTITIES.—No cause of action shall lie or be maintained in any court against any entity for—

(i) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(ii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such entity.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed as creating any immunity against, or otherwise affecting, any action brought by the Federal government, or any agency or department thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, and use of classified information.

(h) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this section shall be construed to limit or prohibit otherwise lawful disclosures of communications, records, or other information by a private entity to any other governmental or private entity not covered under this section.

(i) WHISTLEBLOWER PROTECTION.—Nothing in this Act shall be construed to preempt or preclude any employee from exercising rights currently provided under any whistleblower law, rule, or regulation.

(j) RELATIONSHIP TO OTHER LAWS.—The submission of cyber threat information under this section to a cybersecurity center shall not affect any requirement under any other provision of law for an entity to provide information to the Federal government.

SEC. 103. INFORMATION SHARING BY THE FEDERAL GOVERNMENT.

(a) CLASSIFIED INFORMATION.—

(1) PROCEDURES.—Consistent with the protection of intelligence sources and methods, and as otherwise determined appropriate, the Director of National Intelligence and the Secretary of Defense, in consultation with the heads of the appropriate Federal departments or agencies, shall develop and promulgate procedures to facilitate and promote—

(A) the immediate sharing, through the cybersecurity centers, of classified cyber threat information in the possession of the Federal government with appropriately cleared representatives of any appropriate entity; and

(B) the declassification and immediate sharing, through the cybersecurity centers, with any entity or, if appropriate, public availability of cyber threat information in the possession of the Federal government;

(2) HANDLING OF CLASSIFIED INFORMATION.—The procedures developed under paragraph (1) shall ensure that each entity receiving classified cyber threat information pursuant to this section has acknowledged in writing the ongoing obligation to comply with all laws, executive orders, and procedures concerning the appropriate handling, disclosure, or use of classified information.

(b) UNCLASSIFIED CYBER THREAT INFORMATION.—The heads of each department or agency containing a cybersecurity center shall jointly develop and promulgate procedures that ensure that, consistent with the provisions of this section, unclassified, including controlled unclassified, cyber threat information in the possession of the Federal government—

(1) is shared, through the cybersecurity centers, in an immediate and adequate manner with appropriate entities; and

(2) if appropriate, is made publicly available.

(c) DEVELOPMENT OF PROCEDURES.—

(1) IN GENERAL.—The procedures developed under this section shall incorporate, to the greatest extent possible, existing processes utilized by sector specific information sharing and analysis centers.

(2) COORDINATION WITH ENTITIES.—In developing the procedures required under this section, the Director of National Intelligence and the heads of each department or agency containing a cybersecurity center shall coordinate with appropriate entities to ensure that protocols are implemented that will facilitate and promote the sharing of cyber threat information by the Federal government.

(d) ADDITIONAL RESPONSIBILITIES OF CYBERSECURITY CENTERS.—Consistent with section 102, a cybersecurity center shall—

(1) facilitate information sharing, interaction, and collaboration among and between cybersecurity centers and—

(A) other Federal entities;

(B) any entity; and

(C) international partners, in consultation with the Secretary of State;

(2) disseminate timely and actionable cybersecurity threat, vulnerability, mitigation, and warning information, including alerts, advisories, indicators, signatures, and mitigation and response measures, to improve the security and protection of information systems; and

(3) coordinate with other Federal entities, as appropriate, to integrate information from across the Federal government to provide situational awareness of the cybersecurity posture of the United States.

(e) SHARING WITHIN THE FEDERAL GOVERNMENT.—The heads of appropriate Federal departments and agencies shall ensure that cyber threat information in the possession of such Federal departments or agencies that relates to the prevention, investigation, or mitigation of threats to information security across the Federal government is shared effectively with the cybersecurity centers.

(f) SUBMISSION TO CONGRESS.—Not later than 60 days after the date of enactment of this Act, the Director of National Intelligence, in coordination with the appropriate head of a department or an agency containing a cybersecurity center, shall submit the procedures required by this section to Congress.

SEC. 104. CONSTRUCTION.

(a) INFORMATION SHARING RELATIONSHIPS.—Nothing in this title shall be construed—

(1) to limit or modify an existing information sharing relationship;

(2) to prohibit a new information sharing relationship;

(3) to require a new information sharing relationship between any entity and the Federal government, except as specified under section 102(b); or

(4) to modify the authority of a department or agency of the Federal government to protect sources and methods and the national security of the United States.

(b) ANTI-TASKING RESTRICTION.—Nothing in this title shall be construed to permit the Federal government—

(1) to require an entity to share information with the Federal government, except as expressly provided under section 102(b); or

(2) to condition the sharing of cyber threat information with an entity on such entity's provision of cyber threat information to the Federal government.

(c) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this title shall be construed to subject any entity to liability for choosing not to engage in the voluntary activities authorized under this title.

(d) USE AND RETENTION OF INFORMATION.—Nothing in this title shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal government to retain or use any information shared under section 102 for any use other than a use permitted under subsection 102(c)(1).

(e) NO NEW FUNDING.—An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 105. REPORT ON IMPLEMENTATION.

(a) CONTENT OF REPORT.—Not later than 1 year after the date of enactment of this Act, and biennially thereafter, the heads of each department or agency containing a cybersecurity center shall jointly submit, in coordination with the privacy and civil liberties officials of such departments or agencies and the Privacy and Civil Liberties Oversight Board, a detailed report to Congress concerning the implementation of this title, including—

(1) an assessment of the sufficiency of the procedures developed under section 103 of this Act in ensuring that cyber threat information in the possession of the Federal government is provided in an immediate and adequate manner to appropriate entities or, if appropriate, is made publicly available;

(2) an assessment of whether information has been appropriately classified and an accounting of the number of security clearances authorized by the Federal government for purposes of this title;

(3) a review of the type of cyber threat information shared with a cybersecurity center under section 102 of this Act, including whether such information meets the definition of cyber threat information under section 101, the degree to which such information may impact the privacy and civil liberties of individuals, any appropriate metrics to determine any impact of the sharing of such information with the Federal government on privacy and civil liberties, and the adequacy of any steps taken to reduce such impact;

(4) a review of actions taken by the Federal government based on information provided to a cybersecurity center under section 102 of this Act, including the appropriateness of any subsequent use under section 102(c)(1) of this Act and whether there was inappropriate stovepiping within the Federal government of any such information;

(5) a description of any violations of the requirements of this title by the Federal government;

(6) a classified list of entities that received classified information from the Federal government under section 103 of this Act and a description of any indication that such information may not have been appropriately handled;

(7) a summary of any breach of information security, if known, attributable to a specific failure by any entity or the Federal government to act on cyber threat information in the possession of such entity or the Federal government that resulted in substantial economic harm or injury to a specific entity or the Federal government; and

(8) any recommendation for improvements or modifications to the authorities under this title.

(b) FORM OF REPORT.—The report under subsection (a) shall be submitted in unclassified form, but shall include a classified annex.

SEC. 106. INSPECTOR GENERAL REVIEW.

(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency are authorized to review compliance by the cybersecurity centers, and by any Federal department or agency receiving cyber threat information from such cybersecurity centers, with the procedures required under section 102 of this Act.

(b) SCOPE OF REVIEW.—The review under subsection (a) shall consider whether the Federal government has handled such cyber threat information in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title.

(c) REPORT TO CONGRESS.—Each review conducted under this section shall be provided to Congress not later than 30 days after the date of completion of the review.

SEC. 107. TECHNICAL AMENDMENTS.

Section 552(b) of title 5, United States Code, is amended—

(1) in paragraph (8), by striking ''or'';

(2) in paragraph (9), by striking ''wells.'' and inserting ''wells; or''; and

(3) by adding at the end the following:

''(10) information shared with or provided to a cybersecurity center under section 102 of title I of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012.''.

SEC. 108. ACCESS TO CLASSIFIED INFORMATION.

(a) AUTHORIZATION REQUIRED.—No person shall be provided with access to classified information (as defined in section 6.1 of Executive Order 13526 (50 U.S.C. 435 note; relating to classified national security information)) relating to cyber security threats or cyber security vulnerabilities under this title without the appropriate security clearances.

(b) SECURITY CLEARANCES.—The appropriate Federal agencies or departments shall, consistent with applicable procedures and requirements, and if otherwise deemed appropriate, assist an individual in timely obtaining an appropriate security clearance where such individual has been determined to be eligible for such clearance and has a need-to-know (as defined in section 6.1 of that Executive Order) classified information to carry out this title.

TITLE II—COORDINATION OF FEDERAL INFORMATION SECURITY POLICY

SEC. 201. COORDINATION OF FEDERAL INFORMATION SECURITY POLICY.

(a) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by striking subchapters II and III and inserting the following:

''SUBCHAPTER II—INFORMATION SECURITY

''§ 3551. Purposes

''The purposes of this subchapter are—

''(1) to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

''(2) to recognize the highly networked nature of the current Federal computing environment and provide effective government-wide management of policies, directives, standards, and guidelines, as well as effective and nimble oversight of and response to information security risks, including coordination of information security efforts throughout the Federal civilian, national security, and law enforcement communities;

''(3) to provide for development and maintenance of controls required to protect agency information and information systems and contribute to the overall improvement of agency information security posture;

''(4) to provide for the development of tools and methods to assess and respond to real-time situational risk for Federal information system operations and assets; and

''(5) to provide a mechanism for improving agency information security programs through continuous monitoring of agency information systems and streamlined reporting requirements rather than overly prescriptive manual reporting.

''§ 3552. Definitions

''In this subchapter:

''(1) ADEQUATE SECURITY.—The term 'adequate security' means security commensurate with the risk and magnitude of the harm resulting from the unauthorized access to or loss, misuse, destruction, or modification of information.

''(2) AGENCY.—The term 'agency' has the meaning given the term in section 3502 of title 44.

''(3) CYBERSECURITY CENTER.—The term 'cybersecurity center' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

''(4) CYBER THREAT INFORMATION.—The term 'cyber threat information' means information that indicates or describes—

''(A) a technical or operation vulnerability or a cyber threat mitigation measure;

''(B) an action or operation to mitigate a cyber threat;

''(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

''(D) a method of defeating a technical control;

''(E) a method of defeating an operational control;

''(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

''(G) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to inadvertently enable the defeat of a technical or operational control;

''(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

''(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

''(J) any combination of subparagraphs (A) through (I).

''(5) DIRECTOR.—The term 'Director' means the Director of the Office of Management and Budget unless otherwise specified.

''(6) ENVIRONMENT OF OPERATION.—The term 'environment of operation' means the information system and environment in which those systems operate, including changing threats, vulnerabilities, technologies, and missions and business practices.

''(7) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

''(8) INCIDENT.—The term 'incident' means an occurrence that—

''(A) actually or imminently jeopardizes the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores, or transmits; or

''(B) constitutes a violation of law or an imminent threat of violation of a law, a security policy, a security procedure, or an acceptable use policy.

''(9) INFORMATION RESOURCES.—The term 'information resources' has the meaning given the term in section 3502 of title 44.

''(10) INFORMATION SECURITY.—The term 'information security' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

''(A) integrity, by guarding against improper information modification or destruction, including by ensuring information non-repudiation and authenticity;

''(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; or

''(C) availability, by ensuring timely and reliable access to and use of information.

''(11) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44.

''(12) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given the term in section 11101 of title 40.

''(13) MALICIOUS RECONNAISSANCE.—The term 'malicious reconnaissance' means a method for actively probing or passively monitoring an information system for the purpose of discerning technical

vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

''(14) NATIONAL SECURITY SYSTEM.—

''(A) IN GENERAL.—The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

''(i) the function, operation, or use of which—

''(I) involves intelligence activities;

''(II) involves cryptologic activities related to national security;

''(III) involves command and control of military forces;

''(IV) involves equipment that is an integral part of a weapon or weapons system; or

''(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

''(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

''(B) LIMITATION.—Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

''(15) OPERATIONAL CONTROL.—The term 'operational control' means a security control for an information system that primarily is implemented and executed by people.

''(16) PERSON.—The term 'person' has the meaning given the term in section 3502 of title 44.

''(17) SECRETARY.—The term 'Secretary' means the Secretary of Commerce unless otherwise specified.

''(18) SECURITY CONTROL.—The term 'security control' means the management, operational, and technical controls, including safeguards or countermeasures, prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

''(19) SIGNIFICANT CYBER INCIDENT.—The term 'significant cyber incident' means a cyber incident resulting in, or an attempted cyber incident that, if successful, would have resulted in—

''(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

''(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

''(20) TECHNICAL CONTROL.—The term 'technical control' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

''§ 3553. Federal information security authority and coordination

''(a) IN GENERAL.—The Secretary, in consultation with the Secretary of Homeland Security, shall—

''(1) issue compulsory and binding policies and directives governing agency information security operations, and require implementation of such policies and directives, including—

''(A) policies and directives consistent with the standards and guidelines promulgated under section 11331 of title 40 to identify and provide information security protections prioritized and commensurate with the risk and impact resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by or on behalf of an agency; or

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(B) minimum operational requirements for Federal Government to protect agency information systems and provide common situational awareness across all agency information systems;

''(C) reporting requirements, consistent with relevant law, regarding information security incidents and cyber threat information;

''(D) requirements for agencywide information security programs;

''(E) performance requirements and metrics for the security of agency information systems;

''(F) training requirements to ensure that agencies are able to fully and timely comply with the policies and directives issued by the Secretary under this subchapter;

''(G) training requirements regarding privacy, civil rights, and civil liberties, and information oversight for agency information security personnel;

''(H) requirements for the annual reports to the Secretary under section 3554(d);

''(I) any other information security operations or information security requirements as determined by the Secretary in coordination with relevant agency heads; and

''(J) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

''(2) review the agencywide information security programs under section 3554; and

''(3) designate an individual or an entity at each cybersecurity center, among other responsibilities—

''(A) to receive reports and information about information security incidents, cyber threat information, and deterioration of security control affecting agency information systems; and

''(B) to act on or share the information under subparagraph (A) in accordance with this subchapter.

''(b) CONSIDERATIONS.—When issuing policies and directives under subsection (a), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology under section 11331 of title 40.

''(c) LIMITATION OF AUTHORITY.—The authorities of the Secretary under this section shall not apply to national security systems. Information security policies, directives, standards and guidelines for national security systems shall be overseen as directed by the President and, in accordance with that direction, carried out under the authority of the heads of agencies that operate or exercise authority over such national security systems.

''(d) STATUTORY CONSTRUCTION.—Nothing in this subchapter shall be construed to alter or amend any law regarding the authority of any head of an agency over such agency.

''§ 3554. Agency responsibilities

''(a) IN GENERAL.—The head of each agency shall—

''(1) be responsible for—

''(A) complying with the policies and directives issued under section 3553;

''(B) providing information security protections commensurate with the risk resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by the agency or by a contractor of an agency or other organization on behalf of an agency; and

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(C) complying with the requirements of this subchapter, including—

''(i) information security standards and guidelines promulgated under section 11331 of title 40;

''(ii) for any national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued as directed by the President; and

''(iii) for any non-national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued under section 3553;

''(D) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

''(E) reporting and sharing, for an agency operating or exercising control of a national security system, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for national security systems issued as directed by the President; and

''(F) reporting and sharing, for those agencies operating or exercising control of non-national security systems, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for non-national security systems as prescribed under section 3553(a), including information to assist the entity designated under section 3555(a) with the ongoing security analysis under section 3555;

''(2) ensure that each senior agency official provides information security for the information and information systems that support the operations and assets under the senior agency official's control, including by—

''(A) assessing the risk and impact that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

''(B) determining the level of information security appropriate to protect such information and information systems in accordance with policies and directives issued under section 3553(a), and standards and guidelines promulgated under section 11331 of title 40 for information security classifications and related requirements;

''(C) implementing policies, procedures, and capabilities to reduce risks to an acceptable level in a cost-effective manner;

''(D) actively monitoring the effective implementation of information security controls and techniques; and

''(E) reporting information about information security incidents, cyber threat information, and deterioration of security controls in a timely and adequate manner to the entity designated under section 3553(a)(3) in accordance with paragraph (1);

''(3) assess and maintain the resiliency of information technology systems critical to agency mission and operations;

''(4) designate the agency Inspector General (or an independent entity selected in consultation with the Director and the Council of Inspectors General on Integrity and Efficiency if the agency does not have an Inspector General) to conduct the annual independent evaluation required under section 3556, and allow the agency Inspector General to contract with an independent entity to perform such evaluation;

''(5) delegate to the Chief Information Officer or equivalent (or to a senior agency official who reports to the Chief Information Officer or equivalent)—

''(A) the authority and primary responsibility to implement an agencywide information security program; and

''(B) the authority to provide information security for the information collected and maintained by the agency (or by a contractor, other agency, or other source on behalf of the agency) and for the information systems that support the operations, assets, and mission of the agency (including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency);

''(6) delegate to the appropriate agency official (who is responsible for a particular agency system or subsystem) the responsibility to ensure and enforce compliance with all requirements of the agency's agencywide information security program in coordination with the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5);

''(7) ensure that an agency has trained personnel who have obtained any necessary security clearances to permit them to assist the agency in complying with this subchapter;

''(8) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5), in coordination with other senior agency officials, reports to the agency head on the effectiveness of the agencywide information security program, including the progress of any remedial actions; and

''(9) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5) has the necessary qualifications to administer the functions described in this subchapter and has information security duties as a primary duty of that official.

''(b) CHIEF INFORMATION OFFICERS.—Each Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under subsection (a)(5) shall—

''(1) establish and maintain an enterprise security operations capability that on a continuous basis—

''(A) detects, reports, contains, mitigates, and responds to information security incidents that impair adequate security of the agency's information or information system in a timely manner and in accordance with the policies and directives under section 3553; and

''(B) reports any information security incident under subparagraph (A) to the entity designated under section 3555;

''(2) develop, maintain, and oversee an agencywide information security program;

''(3) develop, maintain, and oversee information security policies, procedures, and control techniques to address applicable requirements, including requirements under section 3553 of this title and section 11331 of title 40; and

''(4) train and oversee the agency personnel who have significant responsibility for information security with respect to that responsibility.

''(c) AGENCYWIDE INFORMATION SECURITY PROGRAMS.—

''(1) IN GENERAL.—Each agencywide information security program under subsection (b)(2) shall include—

''(A) relevant security risk assessments, including technical assessments and others related to the acquisition process;

''(B) security testing commensurate with risk and impact;

''(C) mitigation of deterioration of security controls commensurate with risk and impact;

''(D) risk-based continuous monitoring and threat assessment of the operational status and security of agency information systems to enable evaluation of the effectiveness of and compliance with information security policies, procedures, and practices, including a relevant and appropriate selection of security controls of information systems identified in the inventory under section 3505(c);

''(E) operation of appropriate technical capabilities in order to detect, mitigate, report, and respond to information security incidents, cyber threat information, and deterioration of security controls in a manner that is consistent with the policies and directives under section 3553, including—

''(i) mitigating risks associated with such information security incidents;

''(ii) notifying and consulting with the entity designated under section 3555; and

''(iii) notifying and consulting with, as appropriate—

''(I) law enforcement and the relevant Office of the Inspector General; and

''(II) any other entity, in accordance with law and as directed by the President;

''(F) a process to ensure that remedial action is taken to address any deficiencies in the information security policies, procedures, and practices of the agency; and

''(G) a plan and procedures to ensure the continuity of operations for information systems that support the operations and assets of the agency.

''(2) RISK MANAGEMENT STRATEGIES.—Each agencywide information security program under subsection (b)(2) shall include the development and maintenance of a risk management strategy for information security. The risk management strategy shall include—

''(A) consideration of information security incidents, cyber threat information, and deterioration of security controls; and

''(B) consideration of the consequences that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency;

''(3) POLICIES AND PROCEDURES.—Each agencywide information security program under subsection (b)(2) shall include policies and procedures that—

''(A) are based on the risk management strategy under paragraph (2);

''(B) reduce information security risks to an acceptable level in a cost-effective manner;

''(C) ensure that cost-effective and adequate information security is addressed as part of the acquisition and ongoing management of each agency information system; and

''(D) ensure compliance with—

''(i) this subchapter; and

''(ii) any other applicable requirements.

''(4) TRAINING REQUIREMENTS.—Each agencywide information security program under subsection (b)(2) shall include information security, privacy, civil rights, civil liberties, and information oversight training that meets any applicable requirements under section 3553. The training shall inform each information security personnel that has access to agency information systems (including contractors and other users of information systems that support the operations and assets of the agency) of—

''(A) the information security risks associated with the information security personnel's activities; and

''(B) the individual's responsibility to comply with the agency policies and procedures that reduce the risks under subparagraph (A).

''(d) ANNUAL REPORT.—Each agency shall submit a report annually to the Secretary of Homeland Security on its agencywide information security program and information systems.

''§ 3555. Multiagency ongoing threat assessment

''(a) IMPLEMENTATION.—The Director of the Office of Management and Budget, in coordination with the Secretary of Homeland Security, shall designate an entity to implement ongoing security analysis concerning agency information systems—

''(1) based on cyber threat information;

''(2) based on agency information system and environment of operation changes, including—

''(A) an ongoing evaluation of the information system security controls; and

''(B) the security state, risk level, and environment of operation of an agency information system, including—

''(i) a change in risk level due to a new cyber threat;

''(ii) a change resulting from a new technology;

''(iii) a change resulting from the agency's mission; and

''(iv) a change resulting from the business practice; and

''(3) using automated processes to the maximum extent possible—

''(A) to increase information system security;

''(B) to reduce paper-based reporting requirements; and

''(C) to maintain timely and actionable knowledge of the state of the information system security.

''(b) STANDARDS.—The National Institute of Standards and Technology may promulgate standards, in coordination with the Secretary of Homeland Security, to assist an agency with its duties under this section.

''(c) COMPLIANCE.—The head of each appropriate department and agency shall be responsible for ensuring compliance and implementing necessary procedures to comply with this section. The head of each appropriate department and agency, in consultation with the Director of the Office of Management and Budget and the Secretary of Homeland Security, shall—

''(1) monitor compliance under this section;

''(2) develop a timeline and implement for the department or agency—

''(A) adoption of any technology, system, or method that facilitates continuous monitoring and threat assessments of an agency information system;

''(B) adoption or updating of any technology, system, or method that prevents, detects, or remediates a significant cyber incident to a Federal information system of the department or agency that has impeded, or is reasonably likely to impede, the performance of a critical mission of the department or agency; and

''(C) adoption of any technology, system, or method that satisfies a requirement under this section.

''(d) LIMITATION OF AUTHORITY.—The authorities of the Director of the Office of Management and Budget and of the Secretary of Homeland Security under this section shall not apply to national security systems.

''(e) REPORT.—Not later than 6 months after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Government Accountability Office shall issue a report evaluating each agency's status toward implementing this section.

''§ 3556. Independent evaluations

''(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency, in consultation with the Director and the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense, shall issue and maintain criteria for the timely, cost-effective, risk-based, and independent evaluation of each agencywide information security program (and practices) to determine the effectiveness of the agencywide information security program (and practices). The criteria shall include measures to assess any conflicts of interest in the performance of the evaluation and whether the agencywide information security program includes appropriate safeguards against disclosure of information where such disclosure may adversely affect information security.

''(b) ANNUAL INDEPENDENT EVALUATIONS.—Each agency shall perform an annual independent evaluation of its agencywide information security program (and practices) in accordance with the criteria under subsection (a).

''(c) DISTRIBUTION OF REPORTS.—Not later than 30 days after receiving an independent evaluation under subsection (b), each agency head shall transmit a copy of the independent evaluation to the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense.

''(d) NATIONAL SECURITY SYSTEMS.—Evaluations involving national security systems shall be conducted as directed by President.

''§ 3557. National security systems.

''The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

''(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system; and

''(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President.''.

(b) SAVINGS PROVISIONS.—

(1) POLICY AND COMPLIANCE GUIDANCE.—Policy and compliance guidance issued by the Director before the date of enactment of this Act under section 3543(a)(1) of title 44, United States Code (as in effect on the day before the date of enactment of this Act), shall continue in effect, according to its terms, until modified, terminated, superseded, or repealed pursuant to section 3553(a)(1) of title 44, United States Code.

(2) STANDARDS AND GUIDELINES.—Standards and guidelines issued by the Secretary of Commerce or by the Director before the date of enactment of this Act under section 11331(a)(1) of title 40, United States Code, (as in effect on the day before the date of enactment of this Act) shall continue in effect, according to their terms, until modified, terminated, superseded, or repealed pursuant to section 11331(a)(1) of title 40, United States Code, as amended by this Act.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) CHAPTER ANALYSIS.—The chapter analysis for chapter 35 of title 44, United States Code, is amended—

(A) by striking the items relating to sections 3531 through 3538;

(B) by striking the items relating to sections 3541 through 3549; and

(C) by inserting the following:

''3551. Purposes.
''3552. Definitions.
''3553. Federal information security authority and coordination.
''3554. Agency responsibilities.
''3555. Multiagency ongoing threat assessment.
''3556. Independent evaluations.
''3557. National security systems.''.

(2) OTHER REFERENCES.—

(A) Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(1)(A)) is amended by striking ''section 3532(3)'' and inserting ''section 3552''.

(B) Section 2222(j)(5) of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(C) Section 2223(c)(3) of title 10, United States Code, is amended, by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(D) Section 2315 of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(E) Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended—

(i) in subsection (a)(2), by striking ''section 3532(b)(2)'' and inserting ''section 3552'';

(ii) in subsection (c)(3), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iii) in subsection (d)(1), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iv) in subsection (d)(8) by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(v) in subsection (d)(8), by striking ''submitted to the Director'' and inserting ''submitted to the Secretary'';

(vi) in subsection (e)(2), by striking ''section 3532(1) of such title'' and inserting ''section 3552 of title 44''; and

(vii) in subsection (e)(5), by striking ''section 3532(b)(2) of such title'' and inserting ''section 3552 of title 44''.

(F) Section 8(d)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7406(d)(1)) is amended by striking ''section 3534(b)'' and inserting ''section 3554(b)(2)''.

SEC. 202. MANAGEMENT OF INFORMATION TECHNOLOGY.

(a) IN GENERAL.—Section 11331 of title 40, United States Code, is amended to read as follows:

''§ 11331. Responsibilities for Federal information systems standards

''(a) STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO PRESCRIBE.—Except as provided under paragraph (2), the Secretary of Commerce shall prescribe standards and guidelines pertaining to Federal information systems—

''(A) in consultation with the Secretary of Homeland Security; and

''(B) on the basis of standards and guidelines developed by the National Institute of Standards and Technology under paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)(2) and (a)(3)).

''(2) NATIONAL SECURITY SYSTEMS.—Standards and guidelines for national security systems shall be developed, prescribed, enforced, and overseen as otherwise authorized by law and as directed by the President.

''(b) MANDATORY STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO MAKE MANDATORY STANDARDS AND GUIDELINES.—The Secretary of Commerce shall make standards and guidelines under subsection (a)(1) compulsory and binding to the extent determined necessary by the Secretary of Commerce to improve the efficiency of operation or security of Federal information systems.

''(2) REQUIRED MANDATORY STANDARDS AND GUIDELINES.—

''(A) IN GENERAL.—Standards and guidelines under subsection (a)(1) shall include information security standards that—

''(i) provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)); and

''(ii) are otherwise necessary to improve the security of Federal information and information systems.

''(B) BINDING EFFECT.—Information security standards under subparagraph (A) shall be compulsory and binding.

''(c) EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary of Commerce shall exercise the authority conferred by this section subject to direction by the President and in coordination with the Director.

''(d) APPLICATION OF MORE STRINGENT STANDARDS AND GUIDELINES.—The head of an executive agency may employ standards for the cost-effective information security for information systems within or under the supervision of that agency that are more stringent than the standards and guidelines the Secretary of Commerce prescribes under this section if the more stringent standards and guidelines—

''(1) contain at least the applicable standards and guidelines made compulsory and binding by the Secretary of Commerce; and

''(2) are otherwise consistent with the policies, directives, and implementation memoranda issued under section 3553(a) of title 44.

''(e) DECISIONS ON PROMULGATION OF STANDARDS AND GUIDELINES.—The decision by the Secretary of Commerce regarding the promulgation of any standard or guideline under this section shall occur not later than 6 months after the date of submission of the proposed standard to the Secretary of Commerce by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

''(f) NOTICE AND COMMENT.—A decision by the Secretary of Commerce to significantly modify, or not promulgate, a proposed standard submitted to the Secretary by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) shall be made after the public is given an opportunity to comment on the Secretary's proposed decision.

''(g) DEFINITIONS.—In this section:

''(1) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' has the meaning given the term in section 3552 of title 44.

''(2) INFORMATION SECURITY.—The term 'information security' has the meaning given the term in section 3552 of title 44.

''(3) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given the term in section 3552 of title 44.''.

SEC. 203. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 204. TECHNICAL AND CONFORMING AMENDMENTS.

Section 21(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4(b)) is amended—

(1) in paragraph (2), by striking ''and the Director of the Office of Management and Budget'' and inserting '', the Secretary of Commerce, and the Secretary of Homeland Security''; and

(2) in paragraph (3), by inserting '', the Secretary of Homeland Security,'' after ''the Secretary of Commerce''.

SEC. 205. CLARIFICATION OF AUTHORITIES.

Nothing in this title shall be construed to convey any new regulatory authority to any government entity implementing or complying with any provision of this title.

TITLE III—CRIMINAL PENALTIES

SEC. 301. PENALTIES FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030(c) of title 18, United States Code, is amended to read as follows:

''(c) The punishment for an offense under subsection (a) or (b) of this section is—

''(1) a fine under this title or imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(1) of this section;

''(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than 3 years, or both, in the case of an offense under subsection (a)(2); or

''(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2) of this section, if—

''(i) the offense was committed for purposes of commercial advantage or private financial gain;

''(ii) the offense was committed in the furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States, or of any State; or

''(iii) the value of the information obtained, or that would have been obtained if the offense was completed, exceeds $5,000;

''(3) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(3) of this section;

''(4) a fine under this title or imprisonment of not more than 20 years, or both, in the case of an offense under subsection (a)(4) of this section;

''(5)(A) except as provided in subparagraph (C), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A) of this section, if the offense caused—

''(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

''(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

''(iii) physical injury to any person;

''(iv) a threat to public health or safety;

''(v) damage affecting a computer used by, or on behalf of, an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

''(vi) damage affecting 10 or more protected computers during any 1-year period;

''(B) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(B), if the offense caused a harm provided in clause (i) through (vi) of subparagraph (A) of this subsection;

''(C) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both;

''(D) a fine under this title, imprisonment for not more than 10 years, or both, for any other offense under subsection (a)(5);

''(E) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(6) of this section; or

''(F) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(7) of this section.''.

SEC. 302. TRAFFICKING IN PASSWORDS.

Section 1030(a)(6) of title 18, United States Code, is amended to read as follows:

''(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information or means of access through which a protected computer (as defined in subparagraphs (A) and (B) of subsection (e)(2)) may be accessed without authorization.''.

SEC. 303. CONSPIRACY AND ATTEMPTED COMPUTER FRAUD OFFENSES.

Section 1030(b) of title 18, United States Code, is amended by inserting ''as if for the completed offense'' after ''punished as provided''.

SEC. 304. CRIMINAL AND CIVIL FORFEITURE FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030 of title 18, United States Code, is amended by striking subsections (i) and (j) and inserting the following:

''(i) CRIMINAL FORFEITURE.—

''(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

''(A) such persons interest in any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of such violation; and

''(B) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of such violation.

''(2) The criminal forfeiture of property under this subsection, including any seizure and disposition of the property, and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

''(j) CIVIL FORFEITURE.—

''(1) The following shall be subject to forfeiture to the United States and no property right, real or personal, shall exist in them:

''(A) Any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of any violation of this section, or a conspiracy to violate this section.

''(B) Any property, real or personal, constituting or derived from any gross proceeds obtained directly or indirectly, or any property traceable to such property, as a result of the commission of any violation of this section, or a conspiracy to violate this section.

''(2) Seizures and forfeitures under this subsection shall be governed by the provisions in chapter 46 relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents and other persons as may be designated for that purpose by the Secretary of Homeland Security or the Attorney General.''.

SEC. 305. DAMAGE TO CRITICAL INFRASTRUCTURE COMPUTERS.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

''§ 1030A. Aggravated damage to a critical infrastructure computer

''(a) DEFINITIONS.—In this section—

''(1) the term 'computer' has the meaning given the term in section 1030;

''(2) the term 'critical infrastructure computer' means a computer that manages or controls systems or assets vital to national defense, national security, national economic security, public health or safety, or any combination of those matters, whether publicly or privately owned or operated, including—

''(A) oil and gas production, storage, conversion, and delivery systems;

''(B) water supply systems;

''(C) telecommunication networks;

''(D) electrical power generation and delivery systems;

''(E) finance and banking systems;

''(F) emergency services;

''(G) transportation systems and services; and

''(H) government operations that provide essential services to the public; and

''(3) the term 'damage' has the meaning given the term in section 1030.

''(b) OFFENSE.—It shall be unlawful, during and in relation to a felony violation of section 1030, to knowingly cause or attempt to cause damage to a critical infrastructure computer if the damage results in (or, in the case of an attempt, if completed, would have resulted in) the substantial impairment—

''(1) of the operation of the critical infrastructure computer; or

''(2) of the critical infrastructure associated with the computer.

''(c) PENALTY.—Any person who violates subsection (b) shall be—

''(1) fined under this title;

''(2) imprisoned for not less than 3 years but not more than 20 years; or

''(3) penalized under paragraphs (1) and (2).

''(d) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

''(1) a court shall not place on probation any person convicted of a violation of this section;

''(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment, including any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for a felony violation of section 1030;

''(3) in determining any term of imprisonment to be imposed for a felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The chapter analysis for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

''1030A. Aggravated damage to a critical infrastructure computer.''.

SEC. 306. LIMITATION ON ACTIONS INVOLVING UNAUTHORIZED USE.

Section 1030(e)(6) of title 18, United States Code, is amended by striking ''alter;'' and inserting ''alter, but does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized;''.

SEC. 307. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

TITLE IV—CYBERSECURITY RESEARCH AND DEVELOPMENT

SEC. 401. NATIONAL HIGH-PERFORMANCE COMPUTING PROGRAM PLANNING AND COORDINATION.

(a) GOALS AND PRIORITIES.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(d) GOALS AND PRIORITIES.—The goals and priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include—

''(1) encouraging and supporting mechanisms for interdisciplinary research and development in networking and information technology, including—

''(A) through collaborations across agencies;

''(B) through collaborations across Program Component Areas;

''(C) through collaborations with industry;

''(D) through collaborations with institutions of higher education;

''(E) through collaborations with Federal laboratories (as defined in section 4 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3703)); and

''(F) through collaborations with international organizations;

''(2) addressing national, multi-agency, multi-faceted challenges of national importance; and

''(3) fostering the transfer of research and development results into new technologies and applications for the benefit of society.''.

(b) DEVELOPMENT OF STRATEGIC PLAN.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(e) STRATEGIC PLAN.—

''(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the agencies under subsection (a)(3)(B), working through the National Science and Technology Council and with the assistance of the Office of Science and Technology Policy shall develop a 5-year strategic plan to guide the activities under subsection (a)(1).

''(2) CONTENTS.—The strategic plan shall specify—

''(A) the near-term objectives for the Program;

''(B) the long-term objectives for the Program;

''(C) the anticipated time frame for achieving the near-term objectives;

''(D) the metrics that will be used to assess any progress made toward achieving the near-term objectives and the long-term objectives; and

''(E) how the Program will achieve the goals and priorities under subsection (d).

''(3) IMPLEMENTATION ROADMAP.—

''(A) IN GENERAL.—The agencies under subsection (a)(3)(B) shall develop and annually update an implementation roadmap for the strategic plan.

''(B) REQUIREMENTS.—The information in the implementation roadmap shall be coordinated with the database under section 102(c) and the annual report under section 101(a)(3). The implementation roadmap shall—

''(i) specify the role of each Federal agency in carrying out or sponsoring research and development to meet the research objectives of the strategic plan, including a description of how progress toward the research objectives will be evaluated, with consideration of any relevant recommendations of the advisory committee;

''(ii) specify the funding allocated to each major research objective of the strategic plan and the source of funding by agency for the current fiscal year; and

''(iii) estimate the funding required for each major research objective of the strategic plan for the next 3 fiscal years.

''(4) RECOMMENDATIONS.—The agencies under subsection (a)(3)(B) shall take into consideration when developing the strategic plan under paragraph (1) the recommendations of—

''(A) the advisory committee under subsection (b); and

''(B) the stakeholders under section 102(a)(3).

''(5) REPORT TO CONGRESS.—The Director of the Office of Science and Technology Policy shall transmit the strategic plan under this subsection, including the implementation roadmap and any updates under paragraph (3), to—

''(A) the advisory committee under subsection (b);

''(B) the Committee on Commerce, Science, and Transportation of the Senate; and

''(C) the Committee on Science and Technology of the House of Representatives.''.

(c) PERIODIC REVIEWS.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(f) PERIODIC REVIEWS.—The agencies under subsection (a)(3)(B) shall—

''(1) periodically assess the contents and funding levels of the Program Component Areas and restructure the Program when warranted, taking into consideration any relevant recommendations of the advisory committee under subsection (b); and

''(2) ensure that the Program includes national, multi-agency, multi-faceted research and development activities, including activities described in section 104.''.

(d) ADDITIONAL RESPONSIBILITIES OF DIRECTOR.—Section 101(a)(2) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(2)) is amended—

(1) by redesignating subparagraphs (E) and (F) as subparagraphs (G) and (H), respectively; and

(2) by inserting after subparagraph (D) the following:

''(E) encourage and monitor the efforts of the agencies participating in the Program to allocate the level of resources and management attention necessary—

''(i) to ensure that the strategic plan under subsection (e) is developed and executed effectively; and

''(ii) to ensure that the objectives of the Program are met;

''(F) working with the Office of Management and Budget and in coordination with the creation of the database under section 102(c), direct the Office of Science and Technology Policy and the agencies participating in the Program to establish a mechanism (consistent with existing law) to track all ongoing and completed research and development projects and associated funding;''.

(e) ADVISORY COMMITTEE.—Section 101(b) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(b)) is amended—

(1) in paragraph (1)—

(A) by inserting after the first sentence the following: ''The co-chairs of the advisory committee shall meet the qualifications of committee members and may be members of the Presidents Council of Advisors on Science and Technology.''; and

(B) by striking ''high-performance'' in subparagraph (D) and inserting ''high-end''; and

(2) by amending paragraph (2) to read as follows:

''(2) In addition to the duties under paragraph (1), the advisory committee shall conduct periodic evaluations of the funding, management, coordination, implementation, and activities of the Program. The advisory committee shall report its findings and recommendations not less frequently than once every 3 fiscal years to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives. The report shall be submitted in conjunction with the update of the strategic plan.''.

(f) REPORT.—Section 101(a)(3) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(3)) is amended—

(1) in subparagraph (C)—

(A) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(B) by striking ''each Program Component Area'' and inserting ''each Program Component Area and each research area supported in accordance with section 104'';

(2) in subparagraph (D)—

(A) by striking ''each Program Component Area,'' and inserting ''each Program Component Area and each research area supported in accordance with section 104,'';

(B) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(C) by striking ''and'' after the semicolon;

(3) by redesignating subparagraph (E) as subparagraph (G); and

(4) by inserting after subparagraph (D) the following:

''(E) include a description of how the objectives for each Program Component Area, and the objectives for activities that involve multiple Program Component Areas, relate to the objectives of the Program identified in the strategic plan under subsection (e);

''(F) include—

''(i) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the next fiscal year by category of activity;

''(ii) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the current fiscal year by category of activity; and

''(iii) the amount of funding provided for the Office of Science and Technology Policy for the current fiscal year by each agency participating in the Program; and''.

(g) DEFINITIONS.—Section 4 of the High-Performance Computing Act of 1991 (15 U.S.C. 5503) is amended—

(1) by redesignating paragraphs (1) and (2) as paragraphs (2) and (3), respectively;

(2) by redesignating paragraph (3) as paragraph (6);

(3) by redesignating paragraphs (6) and (7) as paragraphs (7) and (8), respectively;

(4) by inserting before paragraph (2), as redesignated, the following:

''(1) 'cyber-physical systems' means physical or engineered systems whose networking

and information technology functions and physical elements are deeply integrated and are actively connected to the physical world through sensors, actuators, or other means to perform monitoring and control functions;'';

(5) in paragraph (3), as redesignated, by striking ''high-performance computing'' and inserting ''networking and information technology'';

(6) in paragraph (6), as redesignated—

(A) by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(B) by striking ''supercomputer'' and inserting ''high-end computing'';

(7) in paragraph (5), by striking ''network referred to as'' and all that follows through the semicolon and inserting ''network, including advanced computer networks of Federal agencies and departments''; and

(8) in paragraph (7), as redesignated, by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program''.

SEC. 402. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

(a) RESEARCH IN AREAS OF NATIONAL IMPORTANCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.) is amended by adding at the end the following:

''SEC. 104. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

''(a) IN GENERAL.—The Program shall encourage agencies under section 101(a)(3)(B) to support, maintain, and improve national, multi-agency, multi-faceted, research and development activities in networking and information technology directed toward application areas that have the potential for significant contributions to national economic competitiveness and for other significant societal benefits.

''(b) TECHNICAL SOLUTIONS.—An activity under subsection (a) shall be designed to advance the development of research discoveries by demonstrating technical solutions to important problems in areas including—

''(1) cybersecurity;

''(2) health care;

''(3) energy management and low-power systems and devices;

''(4) transportation, including surface and air transportation;

''(5) cyber-physical systems;

''(6) large-scale data analysis and modeling of physical phenomena;

''(7) large scale data analysis and modeling of behavioral phenomena;

''(8) supply chain quality and security; and

''(9) privacy protection and protected disclosure of confidential data.

''(c) RECOMMENDATIONS.—The advisory committee under section 101(b) shall make recommendations to the Program for candidate research and development areas for support under this section.

''(d) CHARACTERISTICS.—

''(1) IN GENERAL.—Research and development activities under this section—

''(A) shall include projects selected on the basis of applications for support through a competitive, merit-based process;

''(B) shall leverage, when possible, Federal investments through collaboration with related State initiatives;

''(C) shall include a plan for fostering the transfer of research discoveries and the results of technology demonstration activities, including from institutions of higher education and Federal laboratories, to industry for commercial development;

''(D) shall involve collaborations among researchers in institutions of higher education and industry; and

''(E) may involve collaborations among nonprofit research institutions and Federal laboratories, as appropriate.

''(2) COST-SHARING.—In selecting applications for support, the agencies under section 101(a)(3)(B) shall give special consideration to projects that include cost sharing from non-Federal sources.

''(3) MULTIDISCIPLINARY RESEARCH CENTERS.—Research and development activities under this section shall be supported through multidisciplinary research centers, including Federal laboratories, that are organized to investigate basic research questions and carry out technology demonstration activities in areas described in subsection (a). Research may be carried out through existing multidisciplinary centers, including those authorized under section 7024(b)(2) of the America COMPETES Act (42 U.S.C. 1862o–10(2)).''.

(b) CYBER-PHYSICAL SYSTEMS.—Section 101(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following:

''(J) provide for increased understanding of the scientific principles of cyber-physical systems and improve the methods available for the design, development, and operation of cyber-physical systems that are characterized by high reliability, safety, and security; and

''(K) provide for research and development on human-computer interactions, visualization, and big data.''.

(c) TASK FORCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.), as amended by section 402(a) of this Act, is amended by adding at the end the following:

''SEC. 105. TASK FORCE.

''(a) ESTABLISHMENT.—Not later than 180 days after the date of enactment the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy under section 102 shall convene a task force to explore mechanisms for carrying out collaborative research and development activities for cyber-physical systems (including the related technologies required to enable these systems) through a consortium or other appropriate entity with participants from institutions of higher education, Federal laboratories, and industry.

''(b) FUNCTIONS.—The task force shall—

''(1) develop options for a collaborative model and an organizational structure for such entity under which the joint research and development activities could be planned, managed, and conducted effectively, including mechanisms for the allocation of resources among the participants in such entity for support of such activities;

''(2) propose a process for developing a research and development agenda for such entity, including guidelines to ensure an appropriate scope of work focused on nationally significant challenges and requiring collaboration and to ensure the development of related scientific and technological milestones;

''(3) define the roles and responsibilities for the participants from institutions of higher education, Federal laboratories, and industry in such entity;

''(4) propose guidelines for assigning intellectual property rights and for transferring research results to the private sector; and

''(5) make recommendations for how such entity could be funded from Federal, State, and non-governmental sources.

''(c) COMPOSITION.—In establishing the task force under subsection (a), the Director of the Office of Science and Technology Policy shall appoint an equal number of individuals from institutions of higher education and from industry with knowledge and expertise in cyber-physical systems, and may appoint not more than 2 individuals from Federal laboratories.

''(d) REPORT.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy shall transmit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives a report describing the findings and recommendations of the task force.

''(e) TERMINATION.—The task force shall terminate upon transmittal of the report required under subsection (d).

''(f) COMPENSATION AND EXPENSES.—Members of the task force shall serve without compensation.''.

SEC. 403. PROGRAM IMPROVEMENTS.

Section 102 of the High-Performance Computing Act of 1991 (15 U.S.C. 5512) is amended to read as follows:

''SEC. 102. PROGRAM IMPROVEMENTS.

''(a) FUNCTIONS.—The Director of the Office of Science and Technology Policy shall continue—

''(1) to provide technical and administrative support to—

''(A) the agencies participating in planning and implementing the Program, including support needed to develop the strategic plan under section 101(e); and

''(B) the advisory committee under section 101(b);

''(2) to serve as the primary point of contact on Federal networking and information technology activities for government agencies, academia, industry, professional societies, State computing and networking technology programs, interested citizen groups, and others to exchange technical and programmatic information;

''(3) to solicit input and recommendations from a wide range of stakeholders during the development of each strategic plan under section 101(e) by convening at least 1 workshop with invitees from academia, industry, Federal laboratories, and other relevant organizations and institutions;

''(4) to conduct public outreach, including the dissemination of the advisory committee's findings and recommendations, as appropriate;

''(5) to promote access to and early application of the technologies, innovations, and expertise derived from Program activities to agency missions and systems across the Federal Government and to United States industry;

''(6) to ensure accurate and detailed budget reporting of networking and information technology research and development investment; and

''(7) to encourage agencies participating in the Program to use existing programs and resources to strengthen networking and information technology education and training, and increase participation in such fields, including by women and underrepresented minorities.

''(b) SOURCE OF FUNDING.—

''(1) IN GENERAL.—The functions under this section shall be supported by funds from each agency participating in the Program.

''(2) SPECIFICATIONS.—The portion of the total budget of the Office of Science and Technology Policy that is provided by each agency participating in the Program for each

fiscal year shall be in the same proportion as each agency's share of the total budget for the Program for the previous fiscal year, as specified in the database under section 102(c).

''(c) DATABASE.—

''(1) IN GENERAL.—The Director of the Office of Science and Technology Policy shall develop and maintain a database of projects funded by each agency for the fiscal year for each Program Component Area.

''(2) PUBLIC ACCESSIBILITY.—The Director of the Office of Science and Technology Policy shall make the database accessible to the public.

''(3) DATABASE CONTENTS.—The database shall include, for each project in the database—

''(A) a description of the project;

''(B) each agency, industry, institution of higher education, Federal laboratory, or international institution involved in the project;

''(C) the source funding of the project (set forth by agency);

''(D) the funding history of the project; and

''(E) whether the project has been completed.''.

SEC. 404. IMPROVING EDUCATION OF NETWORKING AND INFORMATION TECHNOLOGY, INCLUDING HIGH PERFORMANCE COMPUTING.

Section 201(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)) is amended—

(1) by redesignating paragraphs (2) through (4) as paragraphs (3) through (5), respectively; and

(2) by inserting after paragraph (1) the following:

''(2) the National Science Foundation shall use its existing programs, in collaboration with other agencies, as appropriate, to improve the teaching and learning of networking and information technology at all levels of education and to increase participation in networking and information technology fields;''.

SEC. 405. CONFORMING AND TECHNICAL AMENDMENTS TO THE HIGH-PERFORMANCE COMPUTING ACT OF 1991.

(a) SECTION 3.—Section 3 of the High-Performance Computing Act of 1991 (15 U.S.C. 5502) is amended—

(1) in the matter preceding paragraph (1), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(2) in paragraph (1)—

(A) in the matter preceding subparagraph (A), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(B) in subparagraphs (A), (F), and (G), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(C) in subparagraph (H), by striking ''high-performance'' and inserting ''high-end''; and

(3) in paragraph (2)—

(A) by striking ''high-performance computing and'' and inserting ''networking and information technology, and''; and

(B) by striking ''high-performance computing network'' and inserting ''networking and information technology''.

(b) TITLE HEADING.—The heading of title I of the High-Performance Computing Act of 1991 (105 Stat. 1595) is amended by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''.

(c) SECTION 101.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT**'';

(2) in subsection (a)—

(A) in the subsection heading, by striking ''NATIONAL HIGH-PERFORMANCE COMPUTING'' and inserting ''NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT'';

(B) in paragraph (1)—

(i) by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program'';

(ii) in subparagraph (A), by striking ''high-performance computing, including networking'' and inserting ''networking and information technology'';

(iii) in subparagraphs (B) and (G), by striking ''high-performance'' each place it appears and inserting ''high-end''; and

(iv) in subparagraph (C), by striking ''high-performance computing and networking'' and inserting ''high-end computing, distributed, and networking''; and

(C) in paragraph (2)—

(i) in subparagraphs (A) and (C)—

(I) by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(II) by striking ''development, networking,'' each place it appears and inserting ''development,''; and

(ii) in subparagraphs (G) and (H), as redesignated by section 401(d) of this Act, by striking ''high-performance'' each place it appears and inserting ''high-end'';

(3) in subsection (b)(1), in the matter preceding subparagraph (A), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(4) in subsection (c)(1)(A), by striking ''high-performance computing'' and inserting ''networking and information technology''.

(d) SECTION 201.—Section 201(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)(1)) is amended by striking ''high-performance computing and advanced high-speed computer networking'' and inserting ''networking and information technology research and development''.

(e) SECTION 202.—Section 202(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5522(a)) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(f) SECTION 203.—Section 203(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5523(a)) is amended—

(1) in paragraph (1), by striking ''high-performance computing and networking'' and inserting ''networking and information technology''; and

(2) in paragraph (2)(A), by striking ''high-performance'' and inserting ''high-end''.

(g) SECTION 204.—Section 204 of the High-Performance Computing Act of 1991 (15 U.S.C. 5524) is amended—

(1) in subsection (a)(1)—

(A) in subparagraph (A), by striking ''high-performance computing systems and networks'' and inserting ''networking and information technology systems and capabilities'';

(B) in subparagraph (B), by striking ''interoperability of high-performance computing systems in networks and for common user interfaces to systems'' and inserting ''interoperability and usability of networking and information technology systems''; and

(C) in subparagraph (C), by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(2) in subsection (b)—

(A) by striking ''HIGH-PERFORMANCE COMPUTING AND NETWORK'' in the heading and inserting ''NETWORKING AND INFORMATION TECHNOLOGY''; and

(B) by striking ''sensitive''.

(h) SECTION 205.—Section 205(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5525(a)) is amended by striking ''computational'' and inserting ''networking and information technology''.

(i) SECTION 206.—Section 206(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5526(a)) is amended by striking ''computational research'' and inserting ''networking and information technology research''.

(j) SECTION 207.—Section 207 of the High-Performance Computing Act of 1991 (15 U.S.C. 5527) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(k) SECTION 208.—Section 208 of the High-Performance Computing Act of 1991 (15 U.S.C. 5528) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''; and

(2) in subsection (a)—

(A) in paragraph (1), by striking ''High-performance computing and associated'' and inserting ''Networking and information'';

(B) in paragraph (2), by striking ''high-performance computing'' and inserting ''networking and information technologies'';

(C) in paragraph (3), by striking ''high-performance'' and inserting ''high-end'';

(D) in paragraph (4), by striking ''high-performance computers and associated'' and inserting ''networking and information''; and

(E) in paragraph (5), by striking ''high-performance computing and associated'' and inserting ''networking and information''.

SEC. 406. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation, in coordination with the Secretary of Homeland Security, shall carry out a Federal cyber scholarship-for-service program to recruit and train the next generation of information technology professionals and security managers to meet the needs of the cybersecurity mission for the Federal government.

(b) PROGRAM DESCRIPTION AND COMPONENTS.—The program shall—

(1) annually assess the workforce needs of the Federal government for cybersecurity professionals, including network engineers, software engineers, and other experts in order to determine how many scholarships should be awarded annually to ensure that the workforce needs following graduation match the number of scholarships awarded;

(2) provide scholarships for up to 1,000 students per year in their pursuit of undergraduate or graduate degrees in the cybersecurity field, in an amount that may include coverage for full tuition, fees, and a stipend;

(3) require each scholarship recipient, as a condition of receiving a scholarship under the program, to serve in a Federal information technology workforce for a period equal to one and one-half times each year, or partial year, of scholarship received, in addition to an internship in the cybersecurity field, if applicable, following graduation;

(4) provide a procedure for the National Science Foundation or a Federal agency, consistent with regulations of the Office of Personnel Management, to request and fund a security clearance for a scholarship recipient, including providing for clearance during a summer internship and upon graduation; and

(5) provide opportunities for students to receive temporary appointments for meaningful employment in the Federal information technology workforce during school vacation periods and for internships.

(c) HIRING AUTHORITY.—

(1) IN GENERAL.—For purposes of any law or regulation governing the appointment of an

individual in the Federal civil service, upon the successful completion of the student's studies, a student receiving a scholarship under the program may—

(A) be hired under section 213.3102(r) of title 5, Code of Federal Regulations; and

(B) be exempt from competitive service.

(2) COMPETITIVE SERVICE.—Upon satisfactory fulfillment of the service term under paragraph (1), an individual may be converted to a competitive service position without competition if the individual meets the requirements for that position.

(d) ELIGIBILITY.—The eligibility requirements for a scholarship under this section shall include that a scholarship applicant—

(1) be a citizen of the United States;

(2) be eligible to be granted a security clearance;

(3) maintain a grade point average of 3.2 or above on a 4.0 scale for undergraduate study or a 3.5 or above on a 4.0 scale for postgraduate study;

(4) demonstrate a commitment to a career in improving the security of the information infrastructure; and

(5) has demonstrated a level of proficiency in math or computer sciences.

(e) FAILURE TO COMPLETE SERVICE OBLIGATION.—

(1) IN GENERAL.—A scholarship recipient under this section shall be liable to the United States under paragraph (2) if the scholarship recipient—

(A) fails to maintain an acceptable level of academic standing in the educational institution in which the individual is enrolled, as determined by the Director;

(B) is dismissed from such educational institution for disciplinary reasons;

(C) withdraws from the program for which the award was made before the completion of such program;

(D) declares that the individual does not intend to fulfill the service obligation under this section;

(E) fails to fulfill the service obligation of the individual under this section; or

(F) loses a security clearance or becomes ineligible for a security clearance.

(2) REPAYMENT AMOUNTS.—

(A) LESS THAN 1 YEAR OF SERVICE.—If a circumstance under paragraph (1) occurs before the completion of 1 year of a service obligation under this section, the total amount of awards received by the individual under this section shall be repaid.

(B) ONE OR MORE YEARS OF SERVICE.—If a circumstance described in subparagraph (D) or (E) of paragraph (1) occurs after the completion of 1 year of a service obligation under this section, the total amount of scholarship awards received by the individual under this section, reduced by the ratio of the number of years of service completed divided by the number of years of service required, shall be repaid.

(f) EVALUATION AND REPORT.—The Director of the National Science Foundation shall—

(1) evaluate the success of recruiting individuals for scholarships under this section and of hiring and retaining those individuals in the public sector workforce, including the annual cost and an assessment of how the program actually improves the Federal workforce; and

(2) periodically report the findings under paragraph (1) to Congress.

(g) AUTHORIZATION OF APPROPRIATIONS.—From amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), the Secretary may use funds to carry out the requirements of this section for fiscal years 2012 through 2013.

SEC. 407. STUDY AND ANALYSIS OF CERTIFICATION AND TRAINING OF INFORMATION INFRASTRUCTURE PROFESSIONALS.

(a) STUDY.—The President shall enter into an agreement with the National Academies to conduct a comprehensive study of government, academic, and private-sector accreditation, training, and certification programs for personnel working in information infrastructure. The agreement shall require the National Academies to consult with sector coordinating councils and relevant governmental agencies, regulatory entities, and nongovernmental organizations in the course of the study.

(b) SCOPE.—The study shall include—

(1) an evaluation of the body of knowledge and various skills that specific categories of personnel working in information infrastructure should possess in order to secure information systems;

(2) an assessment of whether existing government, academic, and private-sector accreditation, training, and certification programs provide the body of knowledge and various skills described in paragraph (1);

(3) an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity talent, including barriers relating to compensation, the hiring process, job classification, and hiring flexibility; and

(4) an analysis of the sources and availability of cybersecurity talent, a comparison of the skills and expertise sought by the Federal Government and the private sector, an examination of the current and future capacity of United States institutions of higher education, including community colleges, to provide current and future cybersecurity professionals, through education and training activities, with those skills sought by the Federal Government, State and local entities, and the private sector.

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the National Academies shall submit to the President and Congress a report on the results of the study. The report shall include—

(1) findings regarding the state of information infrastructure accreditation, training, and certification programs, including specific areas of deficiency and demonstrable progress; and

(2) recommendations for the improvement of information infrastructure accreditation, training, and certification programs.

SEC. 408. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

(a) IN GENERAL.—The Director of the National Institute of Standards and Technology, in coordination with appropriate Federal authorities, shall—

(1) as appropriate, ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to Congress a plan for ensuring such Federal agency coordination.

(b) CONSULTATION WITH THE PRIVATE SECTOR.—In carrying out the activities under subsection (a)(1), the Director shall ensure consultation with appropriate private sector stakeholders.

SEC. 409. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

The Director of the National Institute of Standards and Technology shall continue a program to support the development of technical standards, metrology, testbeds, and conformance criteria, taking into account appropriate user concerns—

(1) to improve interoperability among identity management technologies;

(2) to strengthen authentication methods of identity management systems;

(3) to improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols; and

(4) to improve the usability of identity management systems.

SEC. 410. FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY RESEARCH GRANT AREAS.—Section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking ''property.'' and inserting ''property;''; and

(3) by adding at the end the following:

''(J) secure fundamental protocols that are at the heart of inter-network communications and data exchange;

''(K) system security that addresses the building of secure systems from trusted and untrusted components;

''(L) monitoring and detection; and

''(M) resiliency and rapid recovery methods.''.

(b) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY GRANTS.—Section 4(a)(3) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(3)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Secretary finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(c) COMPUTER AND NETWORK SECURITY CENTERS.—Section 4(b)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7403(b)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Secretary finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(d) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—Section 5(a)(6) of the Cyber Security Research and Development Act (15 U.S.C. 7404(a)(6)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Secretary finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT GRANTS.—Section 5(b)(2) of the Cyber Security Research and Development Act (15 U.S.C. 7404(b)(2)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Secretary finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(f) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY RESEARCH.—Section 5(c)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7404(c)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Secretary finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

SA 2607. Mr. MCCAIN (for himself, Mrs. HUTCHISON, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 1, strike line 3 and all that follows through page 211, line 6 and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012'' or ''SECURE IT''.

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

TITLE I—FACILITATING SHARING OF CYBER THREAT INFORMATION

SEC. 101. DEFINITIONS.

In this title:

(1) AGENCY.—The term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code.

(2) ANTITRUST LAWS.—The term ''antitrust laws''—

(A) has the meaning given the term in section 1(a) of the Clayton Act (15 U.S.C. 12(a));

(B) includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that section 5 of that Act applies to unfair methods of competition; and

(C) includes any State law that has the same intent and effect as the laws under subparagraphs (A) and (B).

(3) COUNTERMEASURE.—The term ''countermeasure'' means an automated or a manual action with defensive intent to mitigate cyber threats.

(4) CYBER THREAT INFORMATION.—The term ''cyber threat information'' means information that indicates or describes—

(A) a technical or operation vulnerability or a cyber threat mitigation measure;

(B) an action or operation to mitigate a cyber threat;

(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

(D) a method of defeating a technical control;

(E) a method of defeating an operational control;

(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

(G) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to inadvertently enable the defeat of a technical or operational control;

(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

(J) any combination of subparagraphs (A) through (I).

(5) CYBERSECURITY CENTER.—The term ''cybersecurity center'' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

(6) CYBERSECURITY SYSTEM.—The term ''cybersecurity system'' means a system designed or employed to ensure the integrity, confidentiality, or availability of, or to safeguard, a system or network, including measures intended to protect a system or network from—

(A) efforts to degrade, disrupt, or destroy such system or network; or

(B) theft or misappropriations of private or government information, intellectual property, or personally identifiable information.

(7) ENTITY.—

(A) IN GENERAL.—The term ''entity'' means any private entity, non-Federal government agency or department, or State, tribal, or local government agency or department (including an officer, employee, or agent thereof).

(B) INCLUSIONS.—The term ''entity'' includes a government agency or department (including an officer, employee, or agent thereof) of the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States.

(8) FEDERAL INFORMATION SYSTEM.—The term ''Federal information system'' means an information system of a Federal department or agency used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

(9) INFORMATION SECURITY.—The term ''information security'' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; or

(C) availability, by ensuring timely and reliable access to and use of information.

(10) INFORMATION SYSTEM.—The term ''information system'' has the meaning given the term in section 3502 of title 44, United States Code.

(11) LOCAL GOVERNMENT.—The term ''local government'' means any borough, city, county, parish, town, township, village, or other general purpose political subdivision of a State.

(12) MALICIOUS RECONNAISSANCE.—The term ''malicious reconnaissance'' means a method for actively probing or passively monitoring an information system for the purpose of discerning technical vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(13) OPERATIONAL CONTROL.—The term ''operational control'' means a security control for an information system that primarily is implemented and executed by people.

(14) OPERATIONAL VULNERABILITY.—The term ''operational vulnerability'' means any attribute of policy, process, or procedure that could enable or facilitate the defeat of an operational control.

(15) PRIVATE ENTITY.—The term ''private entity'' means any individual or any private group, organization, or corporation, including an officer, employee, or agent thereof.

(16) SIGNIFICANT CYBER INCIDENT.—The term ''significant cyber incident'' means a cyber incident resulting in, or an attempted cyber incident that, if successful, would have resulted in—

(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

(B) an incident in which an operational or technical control essential to the security or

operation of a Federal information system was defeated.

(17) TECHNICAL CONTROL.—The term ''technical control'' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

(18) TECHNICAL VULNERABILITY.—The term ''technical vulnerability'' means any attribute of hardware or software that could enable or facilitate the defeat of a technical control.

(19) TRIBAL.—The term ''tribal'' has the meaning given the term ''Indian tribe'' in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

SEC. 102. AUTHORIZATION TO SHARE CYBER THREAT INFORMATION.

(a) VOLUNTARY DISCLOSURE.—

(1) PRIVATE ENTITIES.—Notwithstanding any other provision of law, a private entity may, for the purpose of preventing, investigating, or otherwise mitigating threats to information security, on its own networks, or as authorized by another entity, on such entity's networks, employ countermeasures and use cybersecurity systems in order to obtain, identify, or otherwise possess cyber threat information.

(2) ENTITIES.—Notwithstanding any other provision of law, an entity may disclose cyber threat information to—

(A) a cybersecurity center; or

(B) any other entity in order to assist with preventing, investigating, or otherwise mitigating threats to information security.

(3) INFORMATION SECURITY PROVIDERS.—If the cyber threat information described in paragraph (1) is obtained, identified, or otherwise possessed in the course of providing information security products or services under contract to another entity, that entity shall be given, at any time prior to disclosure of such information, a reasonable opportunity to authorize or prevent such disclosure, to request anonymization of such information, or to request that reasonable efforts be made to safeguard such information that identifies specific persons from unauthorized access or disclosure.

(b) SIGNIFICANT CYBER INCIDENTS INVOLVING FEDERAL INFORMATION SYSTEMS.—

(1) IN GENERAL.—An entity providing electronic communication services, remote computing services, or information security services to a Federal department or agency shall inform the Federal department or agency of a significant cyber incident involving the Federal information system of that Federal department or agency that—

(A) is directly known to the entity as a result of providing such services;

(B) is directly related to the provision of such services by the entity; and

(C) as determined by the entity, has impeded or will impede the performance of a critical mission of the Federal department or agency.

(2) ADVANCE COORDINATION.—A Federal department or agency receiving the services described in paragraph (1) shall coordinate in advance with an entity described in paragraph (1) to develop the parameters of any information that may be provided under paragraph (1), including clarification of the type of significant cyber incident that will impede the performance of a critical mission of the Federal department or agency.

(3) REPORT.—A Federal department or agency shall report information provided under this subsection to a cybersecurity center.

(4) CONSTRUCTION.—Any information provided to a cybersecurity center under paragraph (3) shall be treated in the same manner as information provided to a cybersecurity center under subsection (a).

(c) INFORMATION SHARED WITH OR PROVIDED TO A CYBERSECURITY CENTER.—Cyber threat information provided to a cybersecurity center under this section—

(1) may be disclosed to, retained by, and used by, consistent with otherwise applicable Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal government for a cybersecurity purpose, a national security purpose, or in order to prevent, investigate, or prosecute any of the offenses listed in section 2516 of title 18, United States Code, and such information shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under this paragraph;

(2) may, with the prior written consent of the entity submitting such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(3) shall be considered the commercial, financial, or proprietary information of the entity providing such information to the Federal government and any disclosure outside the Federal government may only be made upon the prior written consent by such entity and shall not constitute a waiver of any applicable privilege or protection provided by law, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(4) shall be deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records;

(5) shall be, without discretion, withheld from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records;

(6) shall not be subject to the rules of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official;

(7) shall not, if subsequently provided to a State, tribal, or local government or government agency, otherwise be disclosed or distributed to any entity by such State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent; and

(8) shall not be directly used by any Federal, State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph.

(d) PROCEDURES RELATING TO INFORMATION SHARING WITH A CYBERSECURITY CENTER.—Not later than 60 days after the date of enactment of this Act, the heads of each department or agency containing a cybersecurity center shall jointly develop, promulgate, and submit to Congress procedures to ensure that cyber threat information shared with or provided to—

(1) a cybersecurity center under this section—

(A) may be submitted to a cybersecurity center by an entity, to the greatest extent possible, through a uniform, publicly available process or format that is easily accessible on the website of such cybersecurity center, and that includes the ability to provide relevant details about the cyber threat information and written consent to any subsequent disclosures authorized by this paragraph;

(B) shall immediately be further shared with each cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government;

(C) is handled by the Federal government in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title, and the Federal government may undertake efforts consistent with this subparagraph to limit the impact on privacy and civil liberties of the sharing of cyber threat information with the Federal government; and

(D) except as provided in this section, shall only be used, disclosed, or handled in accordance with the provisions of subsection (c); and

(2) a Federal agency or department under subsection (b) is provided immediately to a cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government.

(e) INFORMATION SHARED BETWEEN ENTITIES.—

(1) IN GENERAL.—An entity sharing cyber threat information with another entity under this title may restrict the use or sharing of such information by such other entity.

(2) FURTHER SHARING.—Cyber threat information shared by any entity with another entity under this title—

(A) shall only be further shared in accordance with any restrictions placed on the sharing of such information by the entity authorizing such sharing, such as appropriate anonymization of such information; and

(B) may not be used by any entity to gain an unfair competitive advantage to the detriment of the entity authorizing the sharing of such information, except that the conduct described in paragraph (3) shall not constitute unfair competitive conduct.

(3) INFORMATION SHARED WITH STATE, TRIBAL, OR LOCAL GOVERNMENT OR GOVERNMENT AGENCY.—Cyber threat information shared with a State, tribal, or local government or government agency under this title—

(A) may, with the prior written consent of the entity sharing such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent;

(B) shall be deemed voluntarily shared information and exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records;

(C) shall not be disclosed or distributed to any entity by the State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any

State, tribal, or local law requiring disclosure of information or records, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent; and

(D) shall not be directly used by any State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this subparagraph.

(4) ANTITRUST EXEMPTION.—The exchange or provision of cyber threat information or assistance between 2 or more private entities under this title shall not be considered a violation of any provision of antitrust laws if exchanged or provided in order to assist with—

(A) facilitating the prevention, investigation, or mitigation of threats to information security; or

(B) communicating or disclosing of cyber threat information to help prevent, investigate or otherwise mitigate the effects of a threat to information security.

(5) NO RIGHT OR BENEFIT.—The provision of cyber threat information to an entity under this section shall not create a right or a benefit to similar information by such entity or any other entity.

(f) FEDERAL PREEMPTION.—

(1) IN GENERAL.—This section supersedes any statute or other law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this section.

(2) STATE LAW ENFORCEMENT.—Nothing in this section shall be construed to supersede any statute or other law of a State or political subdivision of a State concerning the use of authorized law enforcement techniques.

(3) PUBLIC DISCLOSURE.—No information shared with or provided to a State, tribal, or local government or government agency pursuant to this section shall be made publicly available pursuant to any State, tribal, or local law requiring disclosure of information or records.

(g) CIVIL AND CRIMINAL LIABILITY.—

(1) GENERAL PROTECTIONS.—

(A) PRIVATE ENTITIES.—No cause of action shall lie or be maintained in any court against any private entity for—

(i) the use of countermeasures and cybersecurity systems as authorized by this title;

(ii) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(iii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such private entity.

(B) ENTITIES.—No cause of action shall lie or be maintained in any court against any entity for—

(i) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(ii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such entity.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed as creating any immunity against, or otherwise affecting, any action brought by the Federal government, or any agency or department thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, and use of classified information.

(h) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this section shall be construed to limit or prohibit otherwise lawful disclosures of communications, records, or other information by a private entity to any other governmental or private entity not covered under this section.

(i) WHISTLEBLOWER PROTECTION.—Nothing in this Act shall be construed to preempt or preclude any employee from exercising rights currently provided under any whistleblower law, rule, or regulation.

(j) RELATIONSHIP TO OTHER LAWS.—The submission of cyber threat information under this section to a cybersecurity center shall not affect any requirement under any other provision of law for an entity to provide information to the Federal government.

SEC. 103. INFORMATION SHARING BY THE FEDERAL GOVERNMENT.

(a) CLASSIFIED INFORMATION.—

(1) PROCEDURES.—Consistent with the protection of intelligence sources and methods, and as otherwise determined appropriate, the Director of National Intelligence and the Secretary of Defense, in consultation with the heads of the appropriate Federal departments or agencies, shall develop and promulgate procedures to facilitate and promote—

(A) the immediate sharing, through the cybersecurity centers, of classified cyber threat information in the possession of the Federal government with appropriately cleared representatives of any appropriate entity; and

(B) the declassification and immediate sharing, through the cybersecurity centers, with any entity or, if appropriate, public availability of cyber threat information in the possession of the Federal government;

(2) HANDLING OF CLASSIFIED INFORMATION.—The procedures developed under paragraph (1) shall ensure that each entity receiving classified cyber threat information pursuant to this section has acknowledged in writing the ongoing obligation to comply with all laws, executive orders, and procedures concerning the appropriate handling, disclosure, or use of classified information.

(b) UNCLASSIFIED CYBER THREAT INFORMATION.—The heads of each department or agency containing a cybersecurity center shall jointly develop and promulgate procedures that ensure that, consistent with the provisions of this section, unclassified, including controlled unclassified, cyber threat information in the possession of the Federal government—

(1) is shared, through the cybersecurity centers, in an immediate and adequate manner with appropriate entities; and

(2) if appropriate, is made publicly available.

(c) DEVELOPMENT OF PROCEDURES.—

(1) IN GENERAL.—The procedures developed under this section shall incorporate, to the greatest extent possible, existing processes utilized by sector specific information sharing and analysis centers.

(2) COORDINATION WITH ENTITIES.—In developing the procedures required under this section, the Director of National Intelligence and the heads of each department or agency containing a cybersecurity center shall coordinate with appropriate entities to ensure that protocols are implemented that will facilitate and promote the sharing of cyber threat information by the Federal government.

(d) ADDITIONAL RESPONSIBILITIES OF CYBERSECURITY CENTERS.—Consistent with section 102, a cybersecurity center shall—

(1) facilitate information sharing, interaction, and collaboration among and between cybersecurity centers and—

(A) other Federal entities;

(B) any entity; and

(C) international partners, in consultation with the Secretary of State;

(2) disseminate timely and actionable cybersecurity threat, vulnerability, mitigation, and warning information, including alerts, advisories, indicators, signatures, and mitigation and response measures, to improve the security and protection of information systems; and

(3) coordinate with other Federal entities, as appropriate, to integrate information from across the Federal government to provide situational awareness of the cybersecurity posture of the United States.

(e) SHARING WITHIN THE FEDERAL GOVERNMENT.—The heads of appropriate Federal departments and agencies shall ensure that cyber threat information in the possession of such Federal departments or agencies that relates to the prevention, investigation, or mitigation of threats to information security across the Federal government is shared effectively with the cybersecurity centers.

(f) SUBMISSION TO CONGRESS.—Not later than 60 days after the date of enactment of this Act, the Director of National Intelligence, in coordination with the appropriate head of a department or an agency containing a cybersecurity center, shall submit the procedures required by this section to Congress.

SEC. 104. CONSTRUCTION.

(a) INFORMATION SHARING RELATIONSHIPS.—Nothing in this title shall be construed—

(1) to limit or modify an existing information sharing relationship;

(2) to prohibit a new information sharing relationship;

(3) to require a new information sharing relationship between any entity and the Federal government, except as specified under section 102(b); or

(4) to modify the authority of a department or agency of the Federal government to protect sources and methods and the national security of the United States.

(b) ANTI-TASKING RESTRICTION.—Nothing in this title shall be construed to permit the Federal government—

(1) to require an entity to share information with the Federal government, except as expressly provided under section 102(b); or

(2) to condition the sharing of cyber threat information with an entity on such entity's provision of cyber threat information to the Federal government.

(c) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this title shall be construed to subject any entity to liability for choosing not to engage in the voluntary activities authorized under this title.

(d) USE AND RETENTION OF INFORMATION.—Nothing in this title shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal government to retain or use any information shared under section 102 for any use other than a use permitted under subsection 102(c)(1).

(e) NO NEW FUNDING.—An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 105. REPORT ON IMPLEMENTATION.

(a) CONTENT OF REPORT.—Not later than 1 year after the date of enactment of this Act, and biennially thereafter, the heads of each department or agency containing a cybersecurity center shall jointly submit, in coordination with the privacy and civil liberties officials of such departments or agencies and the Privacy and Civil Liberties Oversight Board, a detailed report to Congress concerning the implementation of this title, including—

(1) an assessment of the sufficiency of the procedures developed under section 103 of this Act in ensuring that cyber threat information in the possession of the Federal government is provided in an immediate and adequate manner to appropriate entities or, if appropriate, is made publicly available;

(2) an assessment of whether information has been appropriately classified and an accounting of the number of security clearances authorized by the Federal government for purposes of this title;

(3) a review of the type of cyber threat information shared with a cybersecurity center under section 102 of this Act, including whether such information meets the definition of cyber threat information under section 101, the degree to which such information may impact the privacy and civil liberties of individuals, any appropriate metrics to determine any impact of the sharing of such information with the Federal government on privacy and civil liberties, and the adequacy of any steps taken to reduce such impact;

(4) a review of actions taken by the Federal government based on information provided to a cybersecurity center under section 102 of this Act, including the appropriateness of any subsequent use under section 102(c)(1) of this Act and whether there was inappropriate stovepiping within the Federal government of any such information;

(5) a description of any violations of the requirements of this title by the Federal government;

(6) a classified list of entities that received classified information from the Federal government under section 103 of this Act and a description of any indication that such information may not have been appropriately handled;

(7) a summary of any breach of information security, if known, attributable to a specific failure by any entity or the Federal government to act on cyber threat information in the possession of such entity or the Federal government that resulted in substantial economic harm or injury to a specific entity or the Federal government; and

(8) any recommendation for improvements or modifications to the authorities under this title.

(b) FORM OF REPORT.—The report under subsection (a) shall be submitted in unclassified form, but shall include a classified annex.

SEC. 106. INSPECTOR GENERAL REVIEW.

(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency are authorized to review compliance by the cybersecurity centers, and by any Federal department or agency receiving cyber threat information from such cybersecurity centers, with the procedures required under section 102 of this Act.

(b) SCOPE OF REVIEW.—The review under subsection (a) shall consider whether the Federal government has handled such cyber threat information in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title.

(c) REPORT TO CONGRESS.—Each review conducted under this section shall be provided to Congress not later than 30 days after the date of completion of the review.

SEC. 107. TECHNICAL AMENDMENTS.

Section 552(b) of title 5, United States Code, is amended—

(1) in paragraph (8), by striking ''or'';

(2) in paragraph (9), by striking ''wells.'' and inserting ''wells; or''; and

(3) by adding at the end the following:

''(10) information shared with or provided to a cybersecurity center under section 102 of title I of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012.''.

SEC. 108. ACCESS TO CLASSIFIED INFORMATION.

(a) AUTHORIZATION REQUIRED.—No person shall be provided with access to classified information (as defined in section 6.1 of Executive Order 13526 (50 U.S.C. 435 note; relating to classified national security information)) relating to cyber security threats or cyber security vulnerabilities under this title without the appropriate security clearances.

(b) SECURITY CLEARANCES.—The appropriate Federal agencies or departments shall, consistent with applicable procedures and requirements, and if otherwise deemed appropriate, assist an individual in timely obtaining an appropriate security clearance where such individual has been determined to be eligible for such clearance and has a need-to-know (as defined in section 6.1 of that Executive Order) classified information to carry out this title.

TITLE II—COORDINATION OF FEDERAL INFORMATION SECURITY POLICY

SEC. 201. COORDINATION OF FEDERAL INFORMATION SECURITY POLICY.

(a) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by striking subchapters II and III and inserting the following:

''SUBCHAPTER II—INFORMATION SECURITY

''§ 3551. Purposes

''The purposes of this subchapter are—

''(1) to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

''(2) to recognize the highly networked nature of the current Federal computing environment and provide effective government-wide management of policies, directives, standards, and guidelines, as well as effective and nimble oversight of and response to information security risks, including coordination of information security efforts throughout the Federal civilian, national security, and law enforcement communities;

''(3) to provide for development and maintenance of controls required to protect agency information and information systems and contribute to the overall improvement of agency information security posture;

''(4) to provide for the development of tools and methods to assess and respond to real-time situational risk for Federal information system operations and assets; and

''(5) to provide a mechanism for improving agency information security programs through continuous monitoring of agency information systems and streamlined reporting requirements rather than overly prescriptive manual reporting.

''§ 3552. Definitions

''In this subchapter:

''(1) ADEQUATE SECURITY.—The term 'adequate security' means security commensurate with the risk and magnitude of the harm resulting from the unauthorized access to or loss, misuse, destruction, or modification of information.

''(2) AGENCY.—The term 'agency' has the meaning given the term in section 3502 of title 44.

''(3) CYBERSECURITY CENTER.—The term 'cybersecurity center' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

''(4) CYBER THREAT INFORMATION.—The term 'cyber threat information' means information that indicates or describes—

''(A) a technical or operation vulnerability or a cyber threat mitigation measure;

''(B) an action or operation to mitigate a cyber threat;

''(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

''(D) a method of defeating a technical control;

''(E) a method of defeating an operational control;

''(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

''(G) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to inadvertently enable the defeat of a technical or operational control;

''(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

''(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

''(J) any combination of subparagraphs (A) through (I).

''(5) DIRECTOR.—The term 'Director' means the Director of the Office of Management and Budget unless otherwise specified.

''(6) ENVIRONMENT OF OPERATION.—The term 'environment of operation' means the information system and environment in which those systems operate, including changing threats, vulnerabilities, technologies, and missions and business practices.

''(7) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

''(8) INCIDENT.—The term 'incident' means an occurrence that—

''(A) actually or imminently jeopardizes the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores, or transmits; or

''(B) constitutes a violation of law or an imminent threat of violation of a law, a security policy, a security procedure, or an acceptable use policy.

''(9) INFORMATION RESOURCES.—The term 'information resources' has the meaning given the term in section 3502 of title 44.

''(10) INFORMATION SECURITY.—The term 'information security' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

''(A) integrity, by guarding against improper information modification or destruction, including by ensuring information non-repudiation and authenticity;

''(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; or

''(C) availability, by ensuring timely and reliable access to and use of information.

''(11) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44.

''(12) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given the term in section 11101 of title 40.

''(13) MALICIOUS RECONNAISSANCE.—The term 'malicious reconnaissance' means a method for actively probing or passively monitoring an information system for the purpose of discerning technical

vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

''(14) NATIONAL SECURITY SYSTEM.—

''(A) IN GENERAL.—The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

''(i) the function, operation, or use of which—

''(I) involves intelligence activities;

''(II) involves cryptologic activities related to national security;

''(III) involves command and control of military forces;

''(IV) involves equipment that is an integral part of a weapon or weapons system; or

''(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

''(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

''(B) LIMITATION.—Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

''(15) OPERATIONAL CONTROL.—The term 'operational control' means a security control for an information system that primarily is implemented and executed by people.

''(16) PERSON.—The term 'person' has the meaning given the term in section 3502 of title 44.

''(17) SECRETARY.—The term 'Secretary' means the Secretary of Commerce unless otherwise specified.

''(18) SECURITY CONTROL.—The term 'security control' means the management, operational, and technical controls, including safeguards or countermeasures, prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

''(19) SIGNIFICANT CYBER INCIDENT.—The term 'significant cyber incident' means a cyber incident resulting in, or an attempted cyber incident that, if successful, would have resulted in—

''(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

''(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

''(20) TECHNICAL CONTROL.—The term 'technical control' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

''§ 3553. Federal information security authority and coordination

''(a) IN GENERAL.—The Secretary, in consultation with the Secretary of Homeland Security, shall—

''(1) issue compulsory and binding policies and directives governing agency information security operations, and require implementation of such policies and directives, including—

''(A) policies and directives consistent with the standards and guidelines promulgated under section 11331 of title 40 to identify and provide information security protections prioritized and commensurate with the risk and impact resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by or on behalf of an agency; or

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(B) minimum operational requirements for Federal Government to protect agency information systems and provide common situational awareness across all agency information systems;

''(C) reporting requirements, consistent with relevant law, regarding information security incidents and cyber threat information;

''(D) requirements for agencywide information security programs;

''(E) performance requirements and metrics for the security of agency information systems;

''(F) training requirements to ensure that agencies are able to fully and timely comply with the policies and directives issued by the Secretary under this subchapter;

''(G) training requirements regarding privacy, civil rights, and civil liberties, and information oversight for agency information security personnel;

''(H) requirements for the annual reports to the Secretary under section 3554(d);

''(I) any other information security operations or information security requirements as determined by the Secretary in coordination with relevant agency heads; and

''(J) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

''(2) review the agencywide information security programs under section 3554; and

''(3) designate an individual or an entity at each cybersecurity center, among other responsibilities—

''(A) to receive reports and information about information security incidents, cyber threat information, and deterioration of security control affecting agency information systems; and

''(B) to act on or share the information under subparagraph (A) in accordance with this subchapter.

''(b) CONSIDERATIONS.—When issuing policies and directives under subsection (a), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology under section 11331 of title 40.

''(c) LIMITATION OF AUTHORITY.—The authorities of the Secretary under this section shall not apply to national security systems. Information security policies, directives, standards and guidelines for national security systems shall be overseen as directed by the President and, in accordance with that direction, carried out under the authority of the heads of agencies that operate or exercise authority over such national security systems.

''(d) STATUTORY CONSTRUCTION.—Nothing in this subchapter shall be construed to alter or amend any law regarding the authority of any head of an agency over such agency.

''§ 3554. Agency responsibilities

''(a) IN GENERAL.—The head of each agency shall—

''(1) be responsible for—

''(A) complying with the policies and directives issued under section 3553;

''(B) providing information security protections commensurate with the risk resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by the agency or by a contractor of an agency or other organization on behalf of an agency; and

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(C) complying with the requirements of this subchapter, including—

''(i) information security standards and guidelines promulgated under section 11331 of title 40;

''(ii) for any national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued as directed by the President; and

''(iii) for any non-national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued under section 3553;

''(D) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

''(E) reporting and sharing, for an agency operating or exercising control of a national security system, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for national security systems issued as directed by the President; and

''(F) reporting and sharing, for those agencies operating or exercising control of non-national security systems, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for non-national security systems as prescribed under section 3553(a), including information to assist the entity designated under section 3555(a) with the ongoing security analysis under section 3555;

''(2) ensure that each senior agency official provides information security for the information and information systems that support the operations and assets under the senior agency official's control, including by—

''(A) assessing the risk and impact that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

''(B) determining the level of information security appropriate to protect such information and information systems in accordance with policies and directives issued under section 3553(a), and standards and guidelines promulgated under section 11331 of title 40 for information security classifications and related requirements;

''(C) implementing policies, procedures, and capabilities to reduce risks to an acceptable level in a cost-effective manner;

''(D) actively monitoring the effective implementation of information security controls and techniques; and

''(E) reporting information about information security incidents, cyber threat information, and deterioration of security controls in a timely and adequate manner to the entity designated under section 3553(a)(3) in accordance with paragraph (1);

''(3) assess and maintain the resiliency of information technology systems critical to agency mission and operations;

''(4) designate the agency Inspector General (or an independent entity selected in consultation with the Director and the Council of Inspectors General on Integrity and Efficiency if the agency does not have an Inspector General) to conduct the annual independent evaluation required under section 3556, and allow the agency Inspector General to contract with an independent entity to perform such evaluation;

''(5) delegate to the Chief Information Officer or equivalent (or to a senior agency official who reports to the Chief Information Officer or equivalent)—

''(A) the authority and primary responsibility to implement an agencywide information security program; and

''(B) the authority to provide information security for the information collected and maintained by the agency (or by a contractor, other agency, or other source on behalf of the agency) and for the information systems that support the operations, assets, and mission of the agency (including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency);

''(6) delegate to the appropriate agency official (who is responsible for a particular agency system or subsystem) the responsibility to ensure and enforce compliance with all requirements of the agency's agencywide information security program in coordination with the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5);

''(7) ensure that an agency has trained personnel who have obtained any necessary security clearances to permit them to assist the agency in complying with this subchapter;

''(8) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5), in coordination with other senior agency officials, reports to the agency head on the effectiveness of the agencywide information security program, including the progress of any remedial actions; and

''(9) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5) has the necessary qualifications to administer the functions described in this subchapter and has information security duties as a primary duty of that official.

''(b) CHIEF INFORMATION OFFICERS.—Each Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under subsection (a)(5) shall—

''(1) establish and maintain an enterprise security operations capability that on a continuous basis—

''(A) detects, reports, contains, mitigates, and responds to information security incidents that impair adequate security of the agency's information or information system in a timely manner and in accordance with the policies and directives under section 3553; and

''(B) reports any information security incident under subparagraph (A) to the entity designated under section 3555;

''(2) develop, maintain, and oversee an agencywide information security program;

''(3) develop, maintain, and oversee information security policies, procedures, and control techniques to address applicable requirements, including requirements under section 3553 of this title and section 11331 of title 40; and

''(4) train and oversee the agency personnel who have significant responsibility for information security with respect to that responsibility.

''(c) AGENCYWIDE INFORMATION SECURITY PROGRAMS.—

''(1) IN GENERAL.—Each agencywide information security program under subsection (b)(2) shall include—

''(A) relevant security risk assessments, including technical assessments and others related to the acquisition process;

''(B) security testing commensurate with risk and impact;

''(C) mitigation of deterioration of security controls commensurate with risk and impact;

''(D) risk-based continuous monitoring and threat assessment of the operational status and security of agency information systems to enable evaluation of the effectiveness of and compliance with information security policies, procedures, and practices, including a relevant and appropriate selection of security controls of information systems identified in the inventory under section 3505(c);

''(E) operation of appropriate technical capabilities in order to detect, mitigate, report, and respond to information security incidents, cyber threat information, and deterioration of security controls in a manner that is consistent with the policies and directives under section 3553, including—

''(i) mitigating risks associated with such information security incidents;

''(ii) notifying and consulting with the entity designated under section 3555; and

''(iii) notifying and consulting with, as appropriate—

''(I) law enforcement and the relevant Office of the Inspector General; and

''(II) any other entity, in accordance with law and as directed by the President;

''(F) a process to ensure that remedial action is taken to address any deficiencies in the information security policies, procedures, and practices of the agency; and

''(G) a plan and procedures to ensure the continuity of operations for information systems that support the operations and assets of the agency.

''(2) RISK MANAGEMENT STRATEGIES.—Each agencywide information security program under subsection (b)(2) shall include the development and maintenance of a risk management strategy for information security. The risk management strategy shall include—

''(A) consideration of information security incidents, cyber threat information, and deterioration of security controls; and

''(B) consideration of the consequences that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency;

''(3) POLICIES AND PROCEDURES.—Each agencywide information security program under subsection (b)(2) shall include policies and procedures that—

''(A) are based on the risk management strategy under paragraph (2);

''(B) reduce information security risks to an acceptable level in a cost-effective manner;

''(C) ensure that cost-effective and adequate information security is addressed as part of the acquisition and ongoing management of each agency information system; and

''(D) ensure compliance with—

''(i) this subchapter; and

''(ii) any other applicable requirements.

''(4) TRAINING REQUIREMENTS.—Each agencywide information security program under subsection (b)(2) shall include information security, privacy, civil rights, civil liberties, and information oversight training that meets any applicable requirements under section 3553. The training shall inform each information security personnel that has access to agency information systems (including contractors and other users of information systems that support the operations and assets of the agency) of—

''(A) the information security risks associated with the information security personnel's activities; and

''(B) the individual's responsibility to comply with the agency policies and procedures that reduce the risks under subparagraph (A).

''(d) ANNUAL REPORT.—Each agency shall submit a report annually to the Secretary of Homeland Security on its agencywide information security program and information systems.

''§ 3555. Multiagency ongoing threat assessment

''(a) IMPLEMENTATION.—The Director of the Office of Management and Budget, in coordination with the Secretary of Homeland Security, shall designate an entity to implement ongoing security analysis concerning agency information systems—

''(1) based on cyber threat information;

''(2) based on agency information system and environment of operation changes, including—

''(A) an ongoing evaluation of the information system security controls; and

''(B) the security state, risk level, and environment of operation of an agency information system, including—

''(i) a change in risk level due to a new cyber threat;

''(ii) a change resulting from a new technology;

''(iii) a change resulting from the agency's mission; and

''(iv) a change resulting from the business practice; and

''(3) using automated processes to the maximum extent possible—

''(A) to increase information system security;

''(B) to reduce paper-based reporting requirements; and

''(C) to maintain timely and actionable knowledge of the state of the information system security.

''(b) STANDARDS.—The National Institute of Standards and Technology may promulgate standards, in coordination with the Secretary of Homeland Security, to assist an agency with its duties under this section.

''(c) COMPLIANCE.—The head of each appropriate department and agency shall be responsible for ensuring compliance and implementing necessary procedures to comply with this section. The head of each appropriate department and agency, in consultation with the Director of the Office of Management and Budget and the Secretary of Homeland Security, shall—

''(1) monitor compliance under this section;

''(2) develop a timeline and implement for the department or agency—

''(A) adoption of any technology, system, or method that facilitates continuous monitoring and threat assessments of an agency information system;

''(B) adoption or updating of any technology, system, or method that prevents, detects, or remediates a significant cyber incident to a Federal information system of the department or agency that has impeded, or is reasonably likely to impede, the performance of a critical mission of the department or agency; and

''(C) adoption of any technology, system, or method that satisfies a requirement under this section.

''(d) LIMITATION OF AUTHORITY.—The authorities of the Director of the Office of Management and Budget and of the Secretary of Homeland Security under this section shall not apply to national security systems.

''(e) REPORT.—Not later than 6 months after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Government Accountability Office shall issue a report evaluating each agency's status toward implementing this section.

''§ 3556. Independent evaluations

''(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency, in consultation with the Director and the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense, shall issue and maintain criteria for the timely, cost-effective, risk-based, and independent evaluation of each agencywide information security program (and practices) to determine the effectiveness of the agencywide information security program (and practices). The criteria shall include measures to assess any conflicts of interest in the performance of the evaluation and whether the agencywide information security program includes appropriate safeguards against disclosure of information where such disclosure may adversely affect information security.

''(b) ANNUAL INDEPENDENT EVALUATIONS.—Each agency shall perform an annual independent evaluation of its agencywide information security program (and practices) in accordance with the criteria under subsection (a).

''(c) DISTRIBUTION OF REPORTS.—Not later than 30 days after receiving an independent evaluation under subsection (b), each agency head shall transmit a copy of the independent evaluation to the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense.

''(d) NATIONAL SECURITY SYSTEMS.—Evaluations involving national security systems shall be conducted as directed by President.

''§ 3557. National security systems.

''The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

''(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system; and

''(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President.''.

(b) SAVINGS PROVISIONS.—

(1) POLICY AND COMPLIANCE GUIDANCE.—Policy and compliance guidance issued by the Director before the date of enactment of this Act under section 3543(a)(1) of title 44, United States Code (as in effect on the day before the date of enactment of this Act), shall continue in effect, according to its terms, until modified, terminated, superseded, or repealed pursuant to section 3553(a)(1) of title 44, United States Code.

(2) STANDARDS AND GUIDELINES.—Standards and guidelines issued by the Secretary of Commerce or by the Director before the date of enactment of this Act under section 11331(a)(1) of title 40, United States Code, (as in effect on the day before the date of enactment of this Act) shall continue in effect, according to their terms, until modified, terminated, superseded, or repealed pursuant to section 11331(a)(1) of title 40, United States Code, as amended by this Act.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) CHAPTER ANALYSIS.—The chapter analysis for chapter 35 of title 44, United States Code, is amended—

(A) by striking the items relating to sections 3531 through 3538;

(B) by striking the items relating to sections 3541 through 3549; and

(C) by inserting the following:

''3551. Purposes.
''3552. Definitions.
''3553. Federal information security authority and coordination.
''3554. Agency responsibilities.
''3555. Multiagency ongoing threat assessment.
''3556. Independent evaluations.
''3557. National security systems.''.

(2) OTHER REFERENCES.—

(A) Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(1)(A)) is amended by striking ''section 3532(3)'' and inserting ''section 3552''.

(B) Section 2222(j)(5) of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(C) Section 2223(c)(3) of title 10, United States Code, is amended, by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(D) Section 2315 of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(E) Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended—

(i) in subsection (a)(2), by striking ''section 3532(b)(2)'' and inserting ''section 3552'';

(ii) in subsection (c)(3), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iii) in subsection (d)(1), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iv) in subsection (d)(8) by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(v) in subsection (d)(8), by striking ''submitted to the Director'' and inserting ''submitted to the Secretary'';

(vi) in subsection (e)(2), by striking ''section 3532(1) of such title'' and inserting ''section 3552 of title 44''; and

(vii) in subsection (e)(5), by striking ''section 3532(b)(2) of such title'' and inserting ''section 3552 of title 44''.

(F) Section 8(d)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7406(d)(1)) is amended by striking ''section 3534(b)'' and inserting ''section 3554(b)(2)''.

SEC. 202. MANAGEMENT OF INFORMATION TECHNOLOGY.

(a) IN GENERAL.—Section 11331 of title 40, United States Code, is amended to read as follows:

''§ 11331. Responsibilities for Federal information systems standards

''(a) STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO PRESCRIBE.—Except as provided under paragraph (2), the Secretary of Commerce shall prescribe standards and guidelines pertaining to Federal information systems—

''(A) in consultation with the Secretary of Homeland Security; and

''(B) on the basis of standards and guidelines developed by the National Institute of Standards and Technology under paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)(2) and (a)(3)).

''(2) NATIONAL SECURITY SYSTEMS.—Standards and guidelines for national security systems shall be developed, prescribed, enforced, and overseen as otherwise authorized by law and as directed by the President.

''(b) MANDATORY STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO MAKE MANDATORY STANDARDS AND GUIDELINES.—The Secretary of Commerce shall make standards and guidelines under subsection (a)(1) compulsory and binding to the extent determined necessary by the Secretary of Commerce to improve the efficiency of operation or security of Federal information systems.

''(2) REQUIRED MANDATORY STANDARDS AND GUIDELINES.—

''(A) IN GENERAL.—Standards and guidelines under subsection (a)(1) shall include information security standards that—

''(i) provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)); and

''(ii) are otherwise necessary to improve the security of Federal information and information systems.

''(B) BINDING EFFECT.—Information security standards under subparagraph (A) shall be compulsory and binding.

''(c) EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary of Commerce shall exercise the authority conferred by this section subject to direction by the President and in coordination with the Director.

''(d) APPLICATION OF MORE STRINGENT STANDARDS AND GUIDELINES.—The head of an executive agency may employ standards for the cost-effective information security for information systems within or under the supervision of that agency that are more stringent than the standards and guidelines the Secretary of Commerce prescribes under this section if the more stringent standards and guidelines—

''(1) contain at least the applicable standards and guidelines made compulsory and binding by the Secretary of Commerce; and

''(2) are otherwise consistent with the policies, directives, and implementation memoranda issued under section 3553(a) of title 44.

''(e) DECISIONS ON PROMULGATION OF STANDARDS AND GUIDELINES.—The decision by the Secretary of Commerce regarding the promulgation of any standard or guideline under this section shall occur not later than 6 months after the date of submission of the proposed standard to the Secretary of Commerce by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

''(f) NOTICE AND COMMENT.—A decision by the Secretary of Commerce to significantly modify, or not promulgate, a proposed standard submitted to the Secretary by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) shall be made after the public is given an opportunity to comment on the Secretary's proposed decision.

''(g) DEFINITIONS.—In this section:

''(1) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' has the meaning given the term in section 3552 of title 44.

''(2) INFORMATION SECURITY.—The term 'information security' has the meaning given the term in section 3552 of title 44.

''(3) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given the term in section 3552 of title 44.''.

SEC. 203. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 204. TECHNICAL AND CONFORMING AMENDMENTS.

Section 21(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4(b)) is amended—

(1) in paragraph (2), by striking ''and the Director of the Office of Management and Budget'' and inserting '', the Secretary of Commerce, and the Secretary of Homeland Security''; and

(2) in paragraph (3), by inserting '', the Secretary of Homeland Security,'' after ''the Secretary of Commerce''.

SEC. 205. CLARIFICATION OF AUTHORITIES.

Nothing in this title shall be construed to convey any new regulatory authority to any government entity implementing or complying with any provision of this title.

TITLE III—CRIMINAL PENALTIES

SEC. 301. PENALTIES FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030(c) of title 18, United States Code, is amended to read as follows:

''(c) The punishment for an offense under subsection (a) or (b) of this section is—

''(1) a fine under this title or imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(1) of this section;

''(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than 3 years, or both, in the case of an offense under subsection (a)(2); or

''(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2) of this section, if—

''(i) the offense was committed for purposes of commercial advantage or private financial gain;

''(ii) the offense was committed in the furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States, or of any State; or

''(iii) the value of the information obtained, or that would have been obtained if the offense was completed, exceeds $5,000;

''(3) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(3) of this section;

''(4) a fine under this title or imprisonment of not more than 20 years, or both, in the case of an offense under subsection (a)(4) of this section;

''(5)(A) except as provided in subparagraph (C), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A) of this section, if the offense caused—

''(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

''(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

''(iii) physical injury to any person;

''(iv) a threat to public health or safety;

''(v) damage affecting a computer used by, or on behalf of, an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

''(vi) damage affecting 10 or more protected computers during any 1-year period;

''(B) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(B), if the offense caused a harm provided in clause (i) through (vi) of subparagraph (A) of this subsection;

''(C) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both;

''(D) a fine under this title, imprisonment for not more than 10 years, or both, for any other offense under subsection (a)(5);

''(E) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(6) of this section; or

''(F) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(7) of this section.''.

SEC. 302. TRAFFICKING IN PASSWORDS.

Section 1030(a)(6) of title 18, United States Code, is amended to read as follows:

''(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information or means of access through which a protected computer (as defined in subparagraphs (A) and (B) of subsection (e)(2)) may be accessed without authorization.''.

SEC. 303. CONSPIRACY AND ATTEMPTED COMPUTER FRAUD OFFENSES.

Section 1030(b) of title 18, United States Code, is amended by inserting ''as if for the completed offense'' after ''punished as provided''.

SEC. 304. CRIMINAL AND CIVIL FORFEITURE FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030 of title 18, United States Code, is amended by striking subsections (i) and (j) and inserting the following:

''(i) CRIMINAL FORFEITURE.—

''(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

''(A) such persons interest in any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of such violation; and

''(B) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of such violation.

''(2) The criminal forfeiture of property under this subsection, including any seizure and disposition of the property, and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

''(j) CIVIL FORFEITURE.—

''(1) The following shall be subject to forfeiture to the United States and no property right, real or personal, shall exist in them:

''(A) Any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of any violation of this section, or a conspiracy to violate this section.

''(B) Any property, real or personal, constituting or derived from any gross proceeds obtained directly or indirectly, or any property traceable to such property, as a result of the commission of any violation of this section, or a conspiracy to violate this section.

''(2) Seizures and forfeitures under this subsection shall be governed by the provisions in chapter 46 relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents and other persons as may be designated for that purpose by the Secretary of Homeland Security or the Attorney General.''.

SEC. 305. DAMAGE TO CRITICAL INFRASTRUCTURE COMPUTERS.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

''§ 1030A. Aggravated damage to a critical infrastructure computer

''(a) DEFINITIONS.—In this section—

''(1) the term 'computer' has the meaning given the term in section 1030;

''(2) the term 'critical infrastructure computer' means a computer that manages or controls systems or assets vital to national defense, national security, national economic security, public health or safety, or any combination of those matters, whether publicly or privately owned or operated, including—

''(A) oil and gas production, storage, conversion, and delivery systems;

''(B) water supply systems;

''(C) telecommunication networks;

''(D) electrical power generation and delivery systems;

''(E) finance and banking systems;

''(F) emergency services;

''(G) transportation systems and services; and

''(H) government operations that provide essential services to the public; and

''(3) the term 'damage' has the meaning given the term in section 1030.

''(b) OFFENSE.—It shall be unlawful, during and in relation to a felony violation of section 1030, to knowingly cause or attempt to cause damage to a critical infrastructure computer if the damage results in (or, in the case of an attempt, if completed, would have resulted in) the substantial impairment—

''(1) of the operation of the critical infrastructure computer; or

''(2) of the critical infrastructure associated with the computer.

''(c) PENALTY.—Any person who violates subsection (b) shall be—

''(1) fined under this title;

''(2) imprisoned for not less than 3 years but not more than 20 years; or

''(3) penalized under paragraphs (1) and (2).

''(d) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

''(1) a court shall not place on probation any person convicted of a violation of this section;

''(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment, including any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for a felony violation of section 1030;

''(3) in determining any term of imprisonment to be imposed for a felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The chapter analysis for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

''1030A. Aggravated damage to a critical infrastructure computer.''.

SEC. 306. LIMITATION ON ACTIONS INVOLVING UNAUTHORIZED USE.

Section 1030(e)(6) of title 18, United States Code, is amended by striking ''alter;'' and inserting ''alter, but does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized;''.

SEC. 307. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

TITLE IV—CYBERSECURITY RESEARCH AND DEVELOPMENT

SEC. 401. NATIONAL HIGH-PERFORMANCE COMPUTING PROGRAM PLANNING AND COORDINATION.

(a) GOALS AND PRIORITIES.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(d) GOALS AND PRIORITIES.—The goals and priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include—

''(1) encouraging and supporting mechanisms for interdisciplinary research and development in networking and information technology, including—

''(A) through collaborations across agencies;

''(B) through collaborations across Program Component Areas;

''(C) through collaborations with industry;

''(D) through collaborations with institutions of higher education;

''(E) through collaborations with Federal laboratories (as defined in section 4 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3703)); and

''(F) through collaborations with international organizations;

''(2) addressing national, multi-agency, multi-faceted challenges of national importance; and

''(3) fostering the transfer of research and development results into new technologies and applications for the benefit of society.''.

(b) DEVELOPMENT OF STRATEGIC PLAN.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(e) STRATEGIC PLAN.—

''(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the agencies under subsection (a)(3)(B), working through the National Science and Technology Council and with the assistance of the Office of Science and Technology Policy shall develop a 5-year strategic plan to guide the activities under subsection (a)(1).

''(2) CONTENTS.—The strategic plan shall specify—

''(A) the near-term objectives for the Program;

''(B) the long-term objectives for the Program;

''(C) the anticipated time frame for achieving the near-term objectives;

''(D) the metrics that will be used to assess any progress made toward achieving the near-term objectives and the long-term objectives; and

''(E) how the Program will achieve the goals and priorities under subsection (d).

''(3) IMPLEMENTATION ROADMAP.—

''(A) IN GENERAL.—The agencies under subsection (a)(3)(B) shall develop and annually update an implementation roadmap for the strategic plan.

''(B) REQUIREMENTS.—The information in the implementation roadmap shall be coordinated with the database under section 102(c) and the annual report under section 101(a)(3). The implementation roadmap shall—

''(i) specify the role of each Federal agency in carrying out or sponsoring research and development to meet the research objectives of the strategic plan, including a description of how progress toward the research objectives will be evaluated, with consideration of any relevant recommendations of the advisory committee;

''(ii) specify the funding allocated to each major research objective of the strategic plan and the source of funding by agency for the current fiscal year; and

''(iii) estimate the funding required for each major research objective of the strategic plan for the next 3 fiscal years.

''(4) RECOMMENDATIONS.—The agencies under subsection (a)(3)(B) shall take into consideration when developing the strategic plan under paragraph (1) the recommendations of—

''(A) the advisory committee under subsection (b); and

''(B) the stakeholders under section 102(a)(3).

''(5) REPORT TO CONGRESS.—The Director of the Office of Science and Technology Policy shall transmit the strategic plan under this subsection, including the implementation roadmap and any updates under paragraph (3), to—

''(A) the advisory committee under subsection (b);

''(B) the Committee on Commerce, Science, and Transportation of the Senate; and

''(C) the Committee on Science and Technology of the House of Representatives.''.

(c) PERIODIC REVIEWS.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(f) PERIODIC REVIEWS.—The agencies under subsection (a)(3)(B) shall—

''(1) periodically assess the contents and funding levels of the Program Component Areas and restructure the Program when warranted, taking into consideration any relevant recommendations of the advisory committee under subsection (b); and

''(2) ensure that the Program includes national, multi-agency, multi-faceted research and development activities, including activities described in section 104.''.

(d) ADDITIONAL RESPONSIBILITIES OF DIRECTOR.—Section 101(a)(2) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(2)) is amended—

(1) by redesignating subparagraphs (E) and (F) as subparagraphs (G) and (H), respectively; and

(2) by inserting after subparagraph (D) the following:

''(E) encourage and monitor the efforts of the agencies participating in the Program to allocate the level of resources and management attention necessary—

''(i) to ensure that the strategic plan under subsection (e) is developed and executed effectively; and

''(ii) to ensure that the objectives of the Program are met;

''(F) working with the Office of Management and Budget and in coordination with the creation of the database under section 102(c), direct the Office of Science and Technology Policy and the agencies participating in the Program to establish a mechanism (consistent with existing law) to track all ongoing and completed research and development projects and associated funding;''.

(e) ADVISORY COMMITTEE.—Section 101(b) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(b)) is amended—

(1) in paragraph (1)—

(A) by inserting after the first sentence the following: ''The co-chairs of the advisory committee shall meet the qualifications of committee members and may be members of the Presidents Council of Advisors on Science and Technology.''; and

(B) by striking ''high-performance'' in subparagraph (D) and inserting ''high-end''; and

(2) by amending paragraph (2) to read as follows:

''(2) In addition to the duties under paragraph (1), the advisory committee shall conduct periodic evaluations of the funding, management, coordination, implementation, and activities of the Program. The advisory committee shall report its findings and recommendations not less frequently than once every 3 fiscal years to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives. The report shall be submitted in conjunction with the update of the strategic plan.''.

(f) REPORT.—Section 101(a)(3) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(3)) is amended—

(1) in subparagraph (C)—

(A) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(B) by striking ''each Program Component Area'' and inserting ''each Program Component Area and each research area supported in accordance with section 104'';

(2) in subparagraph (D)—

(A) by striking ''each Program Component Area,'' and inserting ''each Program Component Area and each research area supported in accordance with section 104,'';

(B) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(C) by striking ''and'' after the semicolon;

(3) by redesignating subparagraph (E) as subparagraph (G); and

(4) by inserting after subparagraph (D) the following:

''(E) include a description of how the objectives for each Program Component Area, and the objectives for activities that involve multiple Program Component Areas, relate to the objectives of the Program identified in the strategic plan under subsection (e);

''(F) include—

''(i) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the next fiscal year by category of activity;

''(ii) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the current fiscal year by category of activity; and

''(iii) the amount of funding provided for the Office of Science and Technology Policy for the current fiscal year by each agency participating in the Program; and''.

(g) DEFINITIONS.—Section 4 of the High-Performance Computing Act of 1991 (15 U.S.C. 5503) is amended—

(1) by redesignating paragraphs (1) and (2) as paragraphs (2) and (3), respectively;

(2) by redesignating paragraph (3) as paragraph (6);

(3) by redesignating paragraphs (6) and (7) as paragraphs (7) and (8), respectively;

(4) by inserting before paragraph (2), as redesignated, the following:

''(1) 'cyber-physical systems' means physical or engineered systems whose networking

and information technology functions and physical elements are deeply integrated and are actively connected to the physical world through sensors, actuators, or other means to perform monitoring and control functions;'';

(5) in paragraph (3), as redesignated, by striking ''high-performance computing'' and inserting ''networking and information technology'';

(6) in paragraph (6), as redesignated—

(A) by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(B) by striking ''supercomputer'' and inserting ''high-end computing'';

(7) in paragraph (5), by striking ''network referred to as'' and all that follows through the semicolon and inserting ''network, including advanced computer networks of Federal agencies and departments''; and

(8) in paragraph (7), as redesignated, by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program''.

SEC. 402. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

(a) RESEARCH IN AREAS OF NATIONAL IMPORTANCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.) is amended by adding at the end the following:

''SEC. 104. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

''(a) IN GENERAL.—The Program shall encourage agencies under section 101(a)(3)(B) to support, maintain, and improve national, multi-agency, multi-faceted, research and development activities in networking and information technology directed toward application areas that have the potential for significant contributions to national economic competitiveness and for other significant societal benefits.

''(b) TECHNICAL SOLUTIONS.—An activity under subsection (a) shall be designed to advance the development of research discoveries by demonstrating technical solutions to important problems in areas including—

''(1) cybersecurity;

''(2) health care;

''(3) energy management and low-power systems and devices;

''(4) transportation, including surface and air transportation;

''(5) cyber-physical systems;

''(6) large-scale data analysis and modeling of physical phenomena;

''(7) large scale data analysis and modeling of behavioral phenomena;

''(8) supply chain quality and security; and

''(9) privacy protection and protected disclosure of confidential data.

''(c) RECOMMENDATIONS.—The advisory committee under section 101(b) shall make recommendations to the Program for candidate research and development areas for support under this section.

''(d) CHARACTERISTICS.—

''(1) IN GENERAL.—Research and development activities under this section—

''(A) shall include projects selected on the basis of applications for support through a competitive, merit-based process;

''(B) shall leverage, when possible, Federal investments through collaboration with related State initiatives;

''(C) shall include a plan for fostering the transfer of research discoveries and the results of technology demonstration activities, including from institutions of higher education and Federal laboratories, to industry for commercial development;

''(D) shall involve collaborations among researchers in institutions of higher education and industry; and

''(E) may involve collaborations among nonprofit research institutions and Federal laboratories, as appropriate.

''(2) COST-SHARING.—In selecting applications for support, the agencies under section 101(a)(3)(B) shall give special consideration to projects that include cost sharing from non-Federal sources.

''(3) MULTIDISCIPLINARY RESEARCH CENTERS.—Research and development activities under this section shall be supported through multidisciplinary research centers, including Federal laboratories, that are organized to investigate basic research questions and carry out technology demonstration activities in areas described in subsection (a). Research may be carried out through existing multidisciplinary centers, including those authorized under section 7024(b)(2) of the America COMPETES Act (42 U.S.C. 1862o–10(2)).''.

(b) CYBER-PHYSICAL SYSTEMS.—Section 101(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following:

''(J) provide for increased understanding of the scientific principles of cyber-physical systems and improve the methods available for the design, development, and operation of cyber-physical systems that are characterized by high reliability, safety, and security; and

''(K) provide for research and development on human-computer interactions, visualization, and big data.''.

(c) TASK FORCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.), as amended by section 402(a) of this Act, is amended by adding at the end the following:

''SEC. 105. TASK FORCE.

''(a) ESTABLISHMENT.—Not later than 180 days after the date of enactment the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy under section 102 shall convene a task force to explore mechanisms for carrying out collaborative research and development activities for cyber-physical systems (including the related technologies required to enable these systems) through a consortium or other appropriate entity with participants from institutions of higher education, Federal laboratories, and industry.

''(b) FUNCTIONS.—The task force shall—

''(1) develop options for a collaborative model and an organizational structure for such entity under which the joint research and development activities could be planned, managed, and conducted effectively, including mechanisms for the allocation of resources among the participants in such entity for support of such activities;

''(2) propose a process for developing a research and development agenda for such entity, including guidelines to ensure an appropriate scope of work focused on nationally significant challenges and requiring collaboration and to ensure the development of related scientific and technological milestones;

''(3) define the roles and responsibilities for the participants from institutions of higher education, Federal laboratories, and industry in such entity;

''(4) propose guidelines for assigning intellectual property rights and for transferring research results to the private sector; and

''(5) make recommendations for how such entity could be funded from Federal, State, and non-governmental sources.

''(c) COMPOSITION.—In establishing the task force under subsection (a), the Director of the Office of Science and Technology Policy shall appoint an equal number of individuals from institutions of higher education and from industry with knowledge and expertise in cyber-physical systems, and may appoint not more than 2 individuals from Federal laboratories.

''(d) REPORT.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy shall transmit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives a report describing the findings and recommendations of the task force.

''(e) TERMINATION.—The task force shall terminate upon transmittal of the report required under subsection (d).

''(f) COMPENSATION AND EXPENSES.—Members of the task force shall serve without compensation.''.

SEC. 403. PROGRAM IMPROVEMENTS.

Section 102 of the High-Performance Computing Act of 1991 (15 U.S.C. 5512) is amended to read as follows:

''SEC. 102. PROGRAM IMPROVEMENTS.

''(a) FUNCTIONS.—The Director of the Office of Science and Technology Policy shall continue—

''(1) to provide technical and administrative support to—

''(A) the agencies participating in planning and implementing the Program, including support needed to develop the strategic plan under section 101(e); and

''(B) the advisory committee under section 101(b);

''(2) to serve as the primary point of contact on Federal networking and information technology activities for government agencies, academia, industry, professional societies, State computing and networking technology programs, interested citizen groups, and others to exchange technical and programmatic information;

''(3) to solicit input and recommendations from a wide range of stakeholders during the development of each strategic plan under section 101(e) by convening at least 1 workshop with invitees from academia, industry, Federal laboratories, and other relevant organizations and institutions;

''(4) to conduct public outreach, including the dissemination of the advisory committee's findings and recommendations, as appropriate;

''(5) to promote access to and early application of the technologies, innovations, and expertise derived from Program activities to agency missions and systems across the Federal Government and to United States industry;

''(6) to ensure accurate and detailed budget reporting of networking and information technology research and development investment; and

''(7) to encourage agencies participating in the Program to use existing programs and resources to strengthen networking and information technology education and training, and increase participation in such fields, including by women and underrepresented minorities.

''(b) SOURCE OF FUNDING.—

''(1) IN GENERAL.—The functions under this section shall be supported by funds from each agency participating in the Program.

''(2) SPECIFICATIONS.—The portion of the total budget of the Office of Science and Technology Policy that is provided by each agency participating in the Program for each

fiscal year shall be in the same proportion as each agency's share of the total budget for the Program for the previous fiscal year, as specified in the database under section 102(c).

''(c) DATABASE.—

''(1) IN GENERAL.—The Director of the Office of Science and Technology Policy shall develop and maintain a database of projects funded by each agency for the fiscal year for each Program Component Area.

''(2) PUBLIC ACCESSIBILITY.—The Director of the Office of Science and Technology Policy shall make the database accessible to the public.

''(3) DATABASE CONTENTS.—The database shall include, for each project in the database—

''(A) a description of the project;

''(B) each agency, industry, institution of higher education, Federal laboratory, or international institution involved in the project;

''(C) the source funding of the project (set forth by agency);

''(D) the funding history of the project; and

''(E) whether the project has been completed.''.

SEC. 404. IMPROVING EDUCATION OF NETWORKING AND INFORMATION TECHNOLOGY, INCLUDING HIGH PERFORMANCE COMPUTING.

Section 201(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)) is amended—

(1) by redesignating paragraphs (2) through (4) as paragraphs (3) through (5), respectively; and

(2) by inserting after paragraph (1) the following:

''(2) the National Science Foundation shall use its existing programs, in collaboration with other agencies, as appropriate, to improve the teaching and learning of networking and information technology at all levels of education and to increase participation in networking and information technology fields;''.

SEC. 405. CONFORMING AND TECHNICAL AMENDMENTS TO THE HIGH-PERFORMANCE COMPUTING ACT OF 1991.

(a) SECTION 3.—Section 3 of the High-Performance Computing Act of 1991 (15 U.S.C. 5502) is amended—

(1) in the matter preceding paragraph (1), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(2) in paragraph (1)—

(A) in the matter preceding subparagraph (A), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(B) in subparagraphs (A), (F), and (G), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(C) in subparagraph (H), by striking ''high-performance'' and inserting ''high-end''; and

(3) in paragraph (2)—

(A) by striking ''high-performance computing and'' and inserting ''networking and information technology, and''; and

(B) by striking ''high-performance computing network'' and inserting ''networking and information technology''.

(b) TITLE HEADING.—The heading of title I of the High-Performance Computing Act of 1991 (105 Stat. 1595) is amended by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''.

(c) SECTION 101.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT**'';

(2) in subsection (a)—

(A) in the subsection heading, by striking ''NATIONAL HIGH-PERFORMANCE COMPUTING'' and inserting ''NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT'';

(B) in paragraph (1)—

(i) by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program'';

(ii) in subparagraph (A), by striking ''high-performance computing, including networking'' and inserting ''networking and information technology'';

(iii) in subparagraphs (B) and (G), by striking ''high-performance'' each place it appears and inserting ''high-end''; and

(iv) in subparagraph (C), by striking ''high-performance computing and networking'' and inserting ''high-end computing, distributed, and networking''; and

(C) in paragraph (2)—

(i) in subparagraphs (A) and (C)—

(I) by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(II) by striking ''development, networking,'' each place it appears and inserting ''development,''; and

(ii) in subparagraphs (G) and (H), as redesignated by section 401(d) of this Act, by striking ''high-performance'' each place it appears and inserting ''high-end'';

(3) in subsection (b)(1), in the matter preceding subparagraph (A), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(4) in subsection (c)(1)(A), by striking ''high-performance computing'' and inserting ''networking and information technology''.

(d) SECTION 201.—Section 201(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)(1)) is amended by striking ''high-performance computing and advanced high-speed computer networking'' and inserting ''networking and information technology research and development''.

(e) SECTION 202.—Section 202(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5522(a)) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(f) SECTION 203.—Section 203(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5523(a)) is amended—

(1) in paragraph (1), by striking ''high-performance computing and networking'' and inserting ''networking and information technology''; and

(2) in paragraph (2)(A), by striking ''high-performance'' and inserting ''high-end''.

(g) SECTION 204.—Section 204 of the High-Performance Computing Act of 1991 (15 U.S.C. 5524) is amended—

(1) in subsection (a)(1)—

(A) in subparagraph (A), by striking ''high-performance computing systems and networks'' and inserting ''networking and information technology systems and capabilities'';

(B) in subparagraph (B), by striking ''interoperability of high-performance computing systems in networks and for common user interfaces to systems'' and inserting ''interoperability and usability of networking and information technology systems''; and

(C) in subparagraph (C), by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(2) in subsection (b)—

(A) by striking ''HIGH-PERFORMANCE COMPUTING AND NETWORK'' in the heading and inserting ''NETWORKING AND INFORMATION TECHNOLOGY''; and

(B) by striking ''sensitive''.

(h) SECTION 205.—Section 205(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5525(a)) is amended by striking ''computational'' and inserting ''networking and information technology''.

(i) SECTION 206.—Section 206(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5526(a)) is amended by striking ''computational research'' and inserting ''networking and information technology research''.

(j) SECTION 207.—Section 207 of the High-Performance Computing Act of 1991 (15 U.S.C. 5527) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(k) SECTION 208.—Section 208 of the High-Performance Computing Act of 1991 (15 U.S.C. 5528) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''; and

(2) in subsection (a)—

(A) in paragraph (1), by striking ''High-performance computing and associated'' and inserting ''Networking and information'';

(B) in paragraph (2), by striking ''high-performance computing'' and inserting ''networking and information technologies'';

(C) in paragraph (3), by striking ''high-performance'' and inserting ''high-end'';

(D) in paragraph (4), by striking ''high-performance computers and associated'' and inserting ''networking and information''; and

(E) in paragraph (5), by striking ''high-performance computing and associated'' and inserting ''networking and information''.

SEC. 406. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation, in coordination with the Secretary of Homeland Security, shall carry out a Federal cyber scholarship-for-service program to recruit and train the next generation of information technology professionals and security managers to meet the needs of the cybersecurity mission for the Federal government.

(b) PROGRAM DESCRIPTION AND COMPONENTS.—The program shall—

(1) annually assess the workforce needs of the Federal government for cybersecurity professionals, including network engineers, software engineers, and other experts in order to determine how many scholarships should be awarded annually to ensure that the workforce needs following graduation match the number of scholarships awarded;

(2) provide scholarships for up to 1,000 students per year in their pursuit of undergraduate or graduate degrees in the cybersecurity field, in an amount that may include coverage for full tuition, fees, and a stipend;

(3) require each scholarship recipient, as a condition of receiving a scholarship under the program, to serve in a Federal information technology workforce for a period equal to one and one-half times each year, or partial year, of scholarship received, in addition to an internship in the cybersecurity field, if applicable, following graduation;

(4) provide a procedure for the National Science Foundation or a Federal agency, consistent with regulations of the Office of Personnel Management, to request and fund a security clearance for a scholarship recipient, including providing for clearance during a summer internship and upon graduation; and

(5) provide opportunities for students to receive temporary appointments for meaningful employment in the Federal information technology workforce during school vacation periods and for internships.

(c) HIRING AUTHORITY.—

(1) IN GENERAL.—For purposes of any law or regulation governing the appointment of an

individual in the Federal civil service, upon the successful completion of the student's studies, a student receiving a scholarship under the program may—

(A) be hired under section 213.3102(r) of title 5, Code of Federal Regulations; and

(B) be exempt from competitive service.

(2) COMPETITIVE SERVICE.—Upon satisfactory fulfillment of the service term under paragraph (1), an individual may be converted to a competitive service position without competition if the individual meets the requirements for that position.

(d) ELIGIBILITY.—The eligibility requirements for a scholarship under this section shall include that a scholarship applicant—

(1) be a citizen of the United States;

(2) be eligible to be granted a security clearance;

(3) maintain a grade point average of 3.2 or above on a 4.0 scale for undergraduate study or a 3.5 or above on a 4.0 scale for postgraduate study;

(4) demonstrate a commitment to a career in improving the security of the information infrastructure; and

(5) has demonstrated a level of proficiency in math or computer sciences.

(e) FAILURE TO COMPLETE SERVICE OBLIGATION.—

(1) IN GENERAL.—A scholarship recipient under this section shall be liable to the United States under paragraph (2) if the scholarship recipient—

(A) fails to maintain an acceptable level of academic standing in the educational institution in which the individual is enrolled, as determined by the Director;

(B) is dismissed from such educational institution for disciplinary reasons;

(C) withdraws from the program for which the award was made before the completion of such program;

(D) declares that the individual does not intend to fulfill the service obligation under this section;

(E) fails to fulfill the service obligation of the individual under this section; or

(F) loses a security clearance or becomes ineligible for a security clearance.

(2) REPAYMENT AMOUNTS.—

(A) LESS THAN 1 YEAR OF SERVICE.—If a circumstance under paragraph (1) occurs before the completion of 1 year of a service obligation under this section, the total amount of awards received by the individual under this section shall be repaid.

(B) ONE OR MORE YEARS OF SERVICE.—If a circumstance described in subparagraph (D) or (E) of paragraph (1) occurs after the completion of 1 year of a service obligation under this section, the total amount of scholarship awards received by the individual under this section, reduced by the ratio of the number of years of service completed divided by the number of years of service required, shall be repaid.

(f) EVALUATION AND REPORT.—The Director of the National Science Foundation shall—

(1) evaluate the success of recruiting individuals for scholarships under this section and of hiring and retaining those individuals in the public sector workforce, including the annual cost and an assessment of how the program actually improves the Federal workforce; and

(2) periodically report the findings under paragraph (1) to Congress.

(g) AUTHORIZATION OF APPROPRIATIONS.—From amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), the Director may use funds to carry out the requirements of this section for fiscal years 2012 through 2013.

SEC. 407. STUDY AND ANALYSIS OF CERTIFICATION AND TRAINING OF INFORMATION INFRASTRUCTURE PROFESSIONALS.

(a) STUDY.—The President shall enter into an agreement with the National Academies to conduct a comprehensive study of government, academic, and private-sector accreditation, training, and certification programs for personnel working in information infrastructure. The agreement shall require the National Academies to consult with sector coordinating councils and relevant governmental agencies, regulatory entities, and nongovernmental organizations in the course of the study.

(b) SCOPE.—The study shall include—

(1) an evaluation of the body of knowledge and various skills that specific categories of personnel working in information infrastructure should possess in order to secure information systems;

(2) an assessment of whether existing government, academic, and private-sector accreditation, training, and certification programs provide the body of knowledge and various skills described in paragraph (1);

(3) an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity talent, including barriers relating to compensation, the hiring process, job classification, and hiring flexibility; and

(4) an analysis of the sources and availability of cybersecurity talent, a comparison of the skills and expertise sought by the Federal Government and the private sector, an examination of the current and future capacity of United States institutions of higher education, including community colleges, to provide current and future cybersecurity professionals, through education and training activities, with those skills sought by the Federal Government, State and local entities, and the private sector.

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the National Academies shall submit to the President and Congress a report on the results of the study. The report shall include—

(1) findings regarding the state of information infrastructure accreditation, training, and certification programs, including specific areas of deficiency and demonstrable progress; and

(2) recommendations for the improvement of information infrastructure accreditation, training, and certification programs.

SEC. 408. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

(a) IN GENERAL.—The Director of the National Institute of Standards and Technology, in coordination with appropriate Federal authorities, shall—

(1) as appropriate, ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to Congress a plan for ensuring such Federal agency coordination.

(b) CONSULTATION WITH THE PRIVATE SECTOR.—In carrying out the activities under subsection (a)(1), the Director shall ensure consultation with appropriate private sector stakeholders.

SEC. 409. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

The Director of the National Institute of Standards and Technology shall continue a program to support the development of technical standards, metrology, testbeds, and conformance criteria, taking into account appropriate user concerns—

(1) to improve interoperability among identity management technologies;

(2) to strengthen authentication methods of identity management systems;

(3) to improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols; and

(4) to improve the usability of identity management systems.

SEC. 410. FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY RESEARCH GRANT AREAS.—Section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking ''property.'' and inserting ''property;''; and

(3) by adding at the end the following:

''(J) secure fundamental protocols that are at the heart of inter-network communications and data exchange;

''(K) system security that addresses the building of secure systems from trusted and untrusted components;

''(L) monitoring and detection; and

''(M) resiliency and rapid recovery methods.''.

(b) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY GRANTS.—Section 4(a)(3) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(3)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(c) COMPUTER AND NETWORK SECURITY CENTERS.—Section 4(b)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7403(b)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(d) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—Section 5(a)(6) of the Cyber Security Research and Development Act (15 U.S.C. 7404(a)(6)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT GRANTS.—Section 5(b)(2) of the Cyber Security Research and Development Act (15 U.S.C. 7404(b)(2)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(f) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY RESEARCH.—Section 5(c)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7404(c)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

SA 2608. Mr. MCCAIN (for himself, Mrs. HUTCHISON, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastrucutre of the United States; which was ordered to lie on the table; as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012'' or ''SECURE IT''.

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

TITLE I—FACILITATING SHARING OF CYBER THREAT INFORMATION

SEC. 101. DEFINITIONS.

In this title:

(1) AGENCY.—The term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code.

(2) ANTITRUST LAWS.—The term ''antitrust laws''—

(A) has the meaning given the term in section 1(a) of the Clayton Act (15 U.S.C. 12(a));

(B) includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that section 5 of that Act applies to unfair methods of competition; and

(C) includes any State law that has the same intent and effect as the laws under subparagraphs (A) and (B).

(3) COUNTERMEASURE.—The term ''countermeasure'' means an automated or a manual action with defensive intent to mitigate cyber threats.

(4) CYBER THREAT INFORMATION.—The term ''cyber threat information'' means information that indicates or describes—

(A) a technical or operation vulnerability or a cyber threat mitigation measure;

(B) an action or operation to mitigate a cyber threat;

(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

(D) a method of defeating a technical control;

(E) a method of defeating an operational control;

(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

(G) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to inadvertently enable the defeat of a technical or operational control;

(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

(J) any combination of subparagraphs (A) through (I).

(5) CYBERSECURITY CENTER.—The term ''cybersecurity center'' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

(6) CYBERSECURITY SYSTEM.—The term ''cybersecurity system'' means a system designed or employed to ensure the integrity, confidentiality, or availability of, or to safeguard, a system or network, including measures intended to protect a system or network from—

(A) efforts to degrade, disrupt, or destroy such system or network; or

(B) theft or misappropriations of private or government information, intellectual property, or personally identifiable information.

(7) ENTITY.—

(A) IN GENERAL.—The term ''entity'' means any private entity, non-Federal government agency or department, or State, tribal, or local government agency or department (including an officer, employee, or agent thereof).

(B) INCLUSIONS.—The term ''entity'' includes a government agency or department (including an officer, employee, or agent thereof) of the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States.

(8) FEDERAL INFORMATION SYSTEM.—The term ''Federal information system'' means an information system of a Federal department or agency used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

(9) INFORMATION SECURITY.—The term ''information security'' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; or

(C) availability, by ensuring timely and reliable access to and use of information.

(10) INFORMATION SYSTEM.—The term ''information system'' has the meaning given the term in section 3502 of title 44, United States Code.

(11) LOCAL GOVERNMENT.—The term ''local government'' means any borough, city, county, parish, town, township, village, or other general purpose political subdivision of a State.

(12) MALICIOUS RECONNAISSANCE.—The term ''malicious reconnaissance'' means a method for actively probing or passively monitoring an information system for the purpose of discerning technical vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(13) OPERATIONAL CONTROL.—The term ''operational control'' means a security control for an information system that primarily is implemented and executed by people.

(14) OPERATIONAL VULNERABILITY.—The term ''operational vulnerability'' means any attribute of policy, process, or procedure that could enable or facilitate the defeat of an operational control.

(15) PRIVATE ENTITY.—The term ''private entity'' means any individual or any private group, organization, or corporation, including an officer, employee, or agent thereof.

(16) SIGNIFICANT CYBER INCIDENT.—The term ''significant cyber incident'' means a cyber incident resulting in, or an attempted cyber incident that, if successful, would have resulted in—

(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

(B) an incident in which an operational or technical control essential to the security or

operation of a Federal information system was defeated.

(17) TECHNICAL CONTROL.—The term ''technical control'' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

(18) TECHNICAL VULNERABILITY.—The term ''technical vulnerability'' means any attribute of hardware or software that could enable or facilitate the defeat of a technical control.

(19) TRIBAL.—The term ''tribal'' has the meaning given the term ''Indian tribe'' in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

SEC. 102. AUTHORIZATION TO SHARE CYBER THREAT INFORMATION.

(a) VOLUNTARY DISCLOSURE.—

(1) PRIVATE ENTITIES.—Notwithstanding any other provision of law, a private entity may, for the purpose of preventing, investigating, or otherwise mitigating threats to information security, on its own networks, or as authorized by another entity, on such entity's networks, employ countermeasures and use cybersecurity systems in order to obtain, identify, or otherwise possess cyber threat information.

(2) ENTITIES.—Notwithstanding any other provision of law, an entity may disclose cyber threat information to—

(A) a cybersecurity center; or

(B) any other entity in order to assist with preventing, investigating, or otherwise mitigating threats to information security.

(3) INFORMATION SECURITY PROVIDERS.—If the cyber threat information described in paragraph (1) is obtained, identified, or otherwise possessed in the course of providing information security products or services under contract to another entity, that entity shall be given, at any time prior to disclosure of such information, a reasonable opportunity to authorize or prevent such disclosure, to request anonymization of such information, or to request that reasonable efforts be made to safeguard such information that identifies specific persons from unauthorized access or disclosure.

(b) SIGNIFICANT CYBER INCIDENTS INVOLVING FEDERAL INFORMATION SYSTEMS.—

(1) IN GENERAL.—An entity providing electronic communication services, remote computing services, or information security services to a Federal department or agency shall inform the Federal department or agency of a significant cyber incident involving the Federal information system of that Federal department or agency that—

(A) is directly known to the entity as a result of providing such services;

(B) is directly related to the provision of such services by the entity; and

(C) as determined by the entity, has impeded or will impede the performance of a critical mission of the Federal department or agency.

(2) ADVANCE COORDINATION.—A Federal department or agency receiving the services described in paragraph (1) shall coordinate in advance with an entity described in paragraph (1) to develop the parameters of any information that may be provided under paragraph (1), including clarification of the type of significant cyber incident that will impede the performance of a critical mission of the Federal department or agency.

(3) REPORT.—A Federal department or agency shall report information provided under this subsection to a cybersecurity center.

(4) CONSTRUCTION.—Any information provided to a cybersecurity center under paragraph (3) shall be treated in the same manner as information provided to a cybersecurity center under subsection (a).

(c) INFORMATION SHARED WITH OR PROVIDED TO A CYBERSECURITY CENTER.—Cyber threat information provided to a cybersecurity center under this section—

(1) may be disclosed to, retained by, and used by, consistent with otherwise applicable Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal government for a cybersecurity purpose, a national security purpose, or in order to prevent, investigate, or prosecute any of the offenses listed in section 2516 of title 18, United States Code, and such information shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under this paragraph;

(2) may, with the prior written consent of the entity submitting such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(3) shall be considered the commercial, financial, or proprietary information of the entity providing such information to the Federal government and any disclosure outside the Federal government may only be made upon the prior written consent by such entity and shall not constitute a waiver of any applicable privilege or protection provided by law, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(4) shall be deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records;

(5) shall be, without discretion, withheld from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records;

(6) shall not be subject to the rules of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official;

(7) shall not, if subsequently provided to a State, tribal, or local government or government agency, otherwise be disclosed or distributed to any entity by such State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent; and

(8) shall not be directly used by any Federal, State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph.

(d) PROCEDURES RELATING TO INFORMATION SHARING WITH A CYBERSECURITY CENTER.—Not later than 60 days after the date of enactment of this Act, the heads of each department or agency containing a cybersecurity center shall jointly develop, promulgate, and submit to Congress procedures to ensure that cyber threat information shared with or provided to—

(1) a cybersecurity center under this section—

(A) may be submitted to a cybersecurity center by an entity, to the greatest extent possible, through a uniform, publicly available process or format that is easily accessible on the website of such cybersecurity center, and that includes the ability to provide relevant details about the cyber threat information and written consent to any subsequent disclosures authorized by this paragraph;

(B) shall immediately be further shared with each cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government;

(C) is handled by the Federal government in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title, and the Federal government may undertake efforts consistent with this subparagraph to limit the impact on privacy and civil liberties of the sharing of cyber threat information with the Federal government; and

(D) except as provided in this section, shall only be used, disclosed, or handled in accordance with the provisions of subsection (c); and

(2) a Federal agency or department under subsection (b) is provided immediately to a cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government.

(e) INFORMATION SHARED BETWEEN ENTITIES.—

(1) IN GENERAL.—An entity sharing cyber threat information with another entity under this title may restrict the use or sharing of such information by such other entity.

(2) FURTHER SHARING.—Cyber threat information shared by any entity with another entity under this title—

(A) shall only be further shared in accordance with any restrictions placed on the sharing of such information by the entity authorizing such sharing, such as appropriate anonymization of such information; and

(B) may not be used by any entity to gain an unfair competitive advantage to the detriment of the entity authorizing the sharing of such information, except that the conduct described in paragraph (3) shall not constitute unfair competitive conduct.

(3) INFORMATION SHARED WITH STATE, TRIBAL, OR LOCAL GOVERNMENT OR GOVERNMENT AGENCY.—Cyber threat information shared with a State, tribal, or local government or government agency under this title—

(A) may, with the prior written consent of the entity sharing such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent;

(B) shall be deemed voluntarily shared information and exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records;

(C) shall not be disclosed or distributed to any entity by the State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any

State, tribal, or local law requiring disclosure of information or records, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent; and

(D) shall not be directly used by any State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this subparagraph.

(4) ANTITRUST EXEMPTION.—The exchange or provision of cyber threat information or assistance between 2 or more private entities under this title shall not be considered a violation of any provision of antitrust laws if exchanged or provided in order to assist with—

(A) facilitating the prevention, investigation, or mitigation of threats to information security; or

(B) communicating or disclosing of cyber threat information to help prevent, investigate or otherwise mitigate the effects of a threat to information security.

(5) NO RIGHT OR BENEFIT.—The provision of cyber threat information to an entity under this section shall not create a right or a benefit to similar information by such entity or any other entity.

(f) FEDERAL PREEMPTION.—

(1) IN GENERAL.—This section supersedes any statute or other law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this section.

(2) STATE LAW ENFORCEMENT.—Nothing in this section shall be construed to supersede any statute or other law of a State or political subdivision of a State concerning the use of authorized law enforcement techniques.

(3) PUBLIC DISCLOSURE.—No information shared with or provided to a State, tribal, or local government or government agency pursuant to this section shall be made publicly available pursuant to any State, tribal, or local law requiring disclosure of information or records.

(g) CIVIL AND CRIMINAL LIABILITY.—

(1) GENERAL PROTECTIONS.—

(A) PRIVATE ENTITIES.—No cause of action shall lie or be maintained in any court against any private entity for—

(i) the use of countermeasures and cybersecurity systems as authorized by this title;

(ii) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(iii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such private entity.

(B) ENTITIES.—No cause of action shall lie or be maintained in any court against any entity for—

(i) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(ii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such entity.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed as creating any immunity against, or otherwise affecting, any action brought by the Federal government, or any agency or department thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, and use of classified information.

(h) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this section shall be construed to limit or prohibit otherwise lawful disclosures of communications, records, or other information by a private entity to any other governmental or private entity not covered under this section.

(i) WHISTLEBLOWER PROTECTION.—Nothing in this Act shall be construed to preempt or preclude any employee from exercising rights currently provided under any whistleblower law, rule, or regulation.

(j) RELATIONSHIP TO OTHER LAWS.—The submission of cyber threat information under this section to a cybersecurity center shall not affect any requirement under any other provision of law for an entity to provide information to the Federal government.

SEC. 103. INFORMATION SHARING BY THE FEDERAL GOVERNMENT.

(a) CLASSIFIED INFORMATION.—

(1) PROCEDURES.—Consistent with the protection of intelligence sources and methods, and as otherwise determined appropriate, the Director of National Intelligence and the Secretary of Defense, in consultation with the heads of the appropriate Federal departments or agencies, shall develop and promulgate procedures to facilitate and promote—

(A) the immediate sharing, through the cybersecurity centers, of classified cyber threat information in the possession of the Federal government with appropriately cleared representatives of any appropriate entity; and

(B) the declassification and immediate sharing, through the cybersecurity centers, with any entity or, if appropriate, public availability of cyber threat information in the possession of the Federal government;

(2) HANDLING OF CLASSIFIED INFORMATION.—The procedures developed under paragraph (1) shall ensure that each entity receiving classified cyber threat information pursuant to this section has acknowledged in writing the ongoing obligation to comply with all laws, executive orders, and procedures concerning the appropriate handling, disclosure, or use of classified information.

(b) UNCLASSIFIED CYBER THREAT INFORMATION.—The heads of each department or agency containing a cybersecurity center shall jointly develop and promulgate procedures that ensure that, consistent with the provisions of this section, unclassified, including controlled unclassified, cyber threat information in the possession of the Federal government—

(1) is shared, through the cybersecurity centers, in an immediate and adequate manner with appropriate entities; and

(2) if appropriate, is made publicly available.

(c) DEVELOPMENT OF PROCEDURES.—

(1) IN GENERAL.—The procedures developed under this section shall incorporate, to the greatest extent possible, existing processes utilized by sector specific information sharing and analysis centers.

(2) COORDINATION WITH ENTITIES.—In developing the procedures required under this section, the Director of National Intelligence and the heads of each department or agency containing a cybersecurity center shall coordinate with appropriate entities to ensure that protocols are implemented that will facilitate and promote the sharing of cyber threat information by the Federal government.

(d) ADDITIONAL RESPONSIBILITIES OF CYBERSECURITY CENTERS.—Consistent with section 102, a cybersecurity center shall—

(1) facilitate information sharing, interaction, and collaboration among and between cybersecurity centers and—

(A) other Federal entities;

(B) any entity; and

(C) international partners, in consultation with the Secretary of State;

(2) disseminate timely and actionable cybersecurity threat, vulnerability, mitigation, and warning information, including alerts, advisories, indicators, signatures, and mitigation and response measures, to improve the security and protection of information systems; and

(3) coordinate with other Federal entities, as appropriate, to integrate information from across the Federal government to provide situational awareness of the cybersecurity posture of the United States.

(e) SHARING WITHIN THE FEDERAL GOVERNMENT.—The heads of appropriate Federal departments and agencies shall ensure that cyber threat information in the possession of such Federal departments or agencies that relates to the prevention, investigation, or mitigation of threats to information security across the Federal government is shared effectively with the cybersecurity centers.

(f) SUBMISSION TO CONGRESS.—Not later than 60 days after the date of enactment of this Act, the Director of National Intelligence, in coordination with the appropriate head of a department or an agency containing a cybersecurity center, shall submit the procedures required by this section to Congress.

SEC. 104. CONSTRUCTION.

(a) INFORMATION SHARING RELATIONSHIPS.—Nothing in this title shall be construed—

(1) to limit or modify an existing information sharing relationship;

(2) to prohibit a new information sharing relationship;

(3) to require a new information sharing relationship between any entity and the Federal government, except as specified under section 102(b); or

(4) to modify the authority of a department or agency of the Federal government to protect sources and methods and the national security of the United States.

(b) ANTI-TASKING RESTRICTION.—Nothing in this title shall be construed to permit the Federal government—

(1) to require an entity to share information with the Federal government, except as expressly provided under section 102(b); or

(2) to condition the sharing of cyber threat information with an entity on such entity's provision of cyber threat information to the Federal government.

(c) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this title shall be construed to subject any entity to liability for choosing not to engage in the voluntary activities authorized under this title.

(d) USE AND RETENTION OF INFORMATION.—Nothing in this title shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal government to retain or use any information shared under section 102 for any use other than a use permitted under subsection 102(c)(1).

(e) NO NEW FUNDING.—An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 105. REPORT ON IMPLEMENTATION.

(a) CONTENT OF REPORT.—Not later than 1 year after the date of enactment of this Act, and biennially thereafter, the heads of each department or agency containing a cybersecurity center shall jointly submit, in coordination with the privacy and civil liberties officials of such departments or agencies and the Privacy and Civil Liberties Oversight Board, a detailed report to Congress concerning the implementation of this title, including—

(1) an assessment of the sufficiency of the procedures developed under section 103 of this Act in ensuring that cyber threat information in the possession of the Federal government is provided in an immediate and adequate manner to appropriate entities or, if appropriate, is made publicly available;

(2) an assessment of whether information has been appropriately classified and an accounting of the number of security clearances authorized by the Federal government for purposes of this title;

(3) a review of the type of cyber threat information shared with a cybersecurity center under section 102 of this Act, including whether such information meets the definition of cyber threat information under section 101, the degree to which such information may impact the privacy and civil liberties of individuals, any appropriate metrics to determine any impact of the sharing of such information with the Federal government on privacy and civil liberties, and the adequacy of any steps taken to reduce such impact;

(4) a review of actions taken by the Federal government based on information provided to a cybersecurity center under section 102 of this Act, including the appropriateness of any subsequent use under section 102(c)(1) of this Act and whether there was inappropriate stovepiping within the Federal government of any such information;

(5) a description of any violations of the requirements of this title by the Federal government;

(6) a classified list of entities that received classified information from the Federal government under section 103 of this Act and a description of any indication that such information may not have been appropriately handled;

(7) a summary of any breach of information security, if known, attributable to a specific failure by any entity or the Federal government to act on cyber threat information in the possession of such entity or the Federal government that resulted in substantial economic harm or injury to a specific entity or the Federal government; and

(8) any recommendation for improvements or modifications to the authorities under this title.

(b) FORM OF REPORT.—The report under subsection (a) shall be submitted in unclassified form, but shall include a classified annex.

SEC. 106. INSPECTOR GENERAL REVIEW.

(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency are authorized to review compliance by the cybersecurity centers, and by any Federal department or agency receiving cyber threat information from such cybersecurity centers, with the procedures required under section 102 of this Act.

(b) SCOPE OF REVIEW.—The review under subsection (a) shall consider whether the Federal government has handled such cyber threat information in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title.

(c) REPORT TO CONGRESS.—Each review conducted under this section shall be provided to Congress not later than 30 days after the date of completion of the review.

SEC. 107. TECHNICAL AMENDMENTS.

Section 552(b) of title 5, United States Code, is amended—

(1) in paragraph (8), by striking ''or'';

(2) in paragraph (9), by striking ''wells.'' and inserting ''wells; or''; and

(3) by adding at the end the following:

''(10) information shared with or provided to a cybersecurity center under section 102 of title I of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012.''.

SEC. 108. ACCESS TO CLASSIFIED INFORMATION.

(a) AUTHORIZATION REQUIRED.—No person shall be provided with access to classified information (as defined in section 6.1 of Executive Order 13526 (50 U.S.C. 435 note; relating to classified national security information)) relating to cyber security threats or cyber security vulnerabilities under this title without the appropriate security clearances.

(b) SECURITY CLEARANCES.—The appropriate Federal agencies or departments shall, consistent with applicable procedures and requirements, and if otherwise deemed appropriate, assist an individual in timely obtaining an appropriate security clearance where such individual has been determined to be eligible for such clearance and has a need-to-know (as defined in section 6.1 of that Executive Order) classified information to carry out this title.

TITLE II—COORDINATION OF FEDERAL INFORMATION SECURITY POLICY

SEC. 201. COORDINATION OF FEDERAL INFORMATION SECURITY POLICY.

(a) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by striking subchapters II and III and inserting the following:

''SUBCHAPTER II—INFORMATION SECURITY

''§ 3551. Purposes

''The purposes of this subchapter are—

''(1) to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

''(2) to recognize the highly networked nature of the current Federal computing environment and provide effective government-wide management of policies, directives, standards, and guidelines, as well as effective and nimble oversight of and response to information security risks, including coordination of information security efforts throughout the Federal civilian, national security, and law enforcement communities;

''(3) to provide for development and maintenance of controls required to protect agency information and information systems and contribute to the overall improvement of agency information security posture;

''(4) to provide for the development of tools and methods to assess and respond to real-time situational risk for Federal information system operations and assets; and

''(5) to provide a mechanism for improving agency information security programs through continuous monitoring of agency information systems and streamlined reporting requirements rather than overly prescriptive manual reporting.

''§ 3552. Definitions

''In this subchapter:

''(1) ADEQUATE SECURITY.—The term 'adequate security' means security commensurate with the risk and magnitude of the harm resulting from the unauthorized access to or loss, misuse, destruction, or modification of information.

''(2) AGENCY.—The term 'agency' has the meaning given the term in section 3502 of title 44.

''(3) CYBERSECURITY CENTER.—The term 'cybersecurity center' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

''(4) CYBER THREAT INFORMATION.—The term 'cyber threat information' means information that indicates or describes—

''(A) a technical or operation vulnerability or a cyber threat mitigation measure;

''(B) an action or operation to mitigate a cyber threat;

''(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

''(D) a method of defeating a technical control;

''(E) a method of defeating an operational control;

''(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

''(G) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to inadvertently enable the defeat of a technical or operational control;

''(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

''(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

''(J) any combination of subparagraphs (A) through (I).

''(5) DIRECTOR.—The term 'Director' means the Director of the Office of Management and Budget unless otherwise specified.

''(6) ENVIRONMENT OF OPERATION.—The term 'environment of operation' means the information system and environment in which those systems operate, including changing threats, vulnerabilities, technologies, and missions and business practices.

''(7) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

''(8) INCIDENT.—The term 'incident' means an occurrence that—

''(A) actually or imminently jeopardizes the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores, or transmits; or

''(B) constitutes a violation of law or an imminent threat of violation of a law, a security policy, a security procedure, or an acceptable use policy.

''(9) INFORMATION RESOURCES.—The term 'information resources' has the meaning given the term in section 3502 of title 44.

''(10) INFORMATION SECURITY.—The term 'information security' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

''(A) integrity, by guarding against improper information modification or destruction, including by ensuring information non-repudiation and authenticity;

''(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; or

''(C) availability, by ensuring timely and reliable access to and use of information.

''(11) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44.

''(12) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given the term in section 11101 of title 40.

''(13) MALICIOUS RECONNAISSANCE.—The term 'malicious reconnaissance' means a method for actively probing or passively monitoring an information system for the purpose of discerning technical

vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

''(14) NATIONAL SECURITY SYSTEM.—

''(A) IN GENERAL.—The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

''(i) the function, operation, or use of which—

''(I) involves intelligence activities;

''(II) involves cryptologic activities related to national security;

''(III) involves command and control of military forces;

''(IV) involves equipment that is an integral part of a weapon or weapons system; or

''(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

''(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

''(B) LIMITATION.—Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

''(15) OPERATIONAL CONTROL.—The term 'operational control' means a security control for an information system that primarily is implemented and executed by people.

''(16) PERSON.—The term 'person' has the meaning given the term in section 3502 of title 44.

''(17) SECRETARY.—The term 'Secretary' means the Secretary of Commerce unless otherwise specified.

''(18) SECURITY CONTROL.—The term 'security control' means the management, operational, and technical controls, including safeguards or countermeasures, prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

''(19) SIGNIFICANT CYBER INCIDENT.—The term 'significant cyber incident' means a cyber incident resulting in, or an attempted cyber incident that, if successful, would have resulted in—

''(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

''(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

''(20) TECHNICAL CONTROL.—The term 'technical control' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

''§ 3553. Federal information security authority and coordination

''(a) IN GENERAL.—The Secretary, in consultation with the Secretary of Homeland Security, shall—

''(1) issue compulsory and binding policies and directives governing agency information security operations, and require implementation of such policies and directives, including—

''(A) policies and directives consistent with the standards and guidelines promulgated under section 11331 of title 40 to identify and provide information security protections prioritized and commensurate with the risk and impact resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by or on behalf of an agency; or

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(B) minimum operational requirements for Federal Government to protect agency information systems and provide common situational awareness across all agency information systems;

''(C) reporting requirements, consistent with relevant law, regarding information security incidents and cyber threat information;

''(D) requirements for agencywide information security programs;

''(E) performance requirements and metrics for the security of agency information systems;

''(F) training requirements to ensure that agencies are able to fully and timely comply with the policies and directives issued by the Secretary under this subchapter;

''(G) training requirements regarding privacy, civil rights, and civil liberties, and information oversight for agency information security personnel;

''(H) requirements for the annual reports to the Secretary under section 3554(d);

''(I) any other information security operations or information security requirements as determined by the Secretary in coordination with relevant agency heads; and

''(J) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

''(2) review the agencywide information security programs under section 3554; and

''(3) designate an individual or an entity at each cybersecurity center, among other responsibilities—

''(A) to receive reports and information about information security incidents, cyber threat information, and deterioration of security control affecting agency information systems; and

''(B) to act on or share the information under subparagraph (A) in accordance with this subchapter.

''(b) CONSIDERATIONS.—When issuing policies and directives under subsection (a), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology under section 11331 of title 40.

''(c) LIMITATION OF AUTHORITY.—The authorities of the Secretary under this section shall not apply to national security systems. Information security policies, directives, standards and guidelines for national security systems shall be overseen as directed by the President and, in accordance with that direction, carried out under the authority of the heads of agencies that operate or exercise authority over such national security systems.

''(d) STATUTORY CONSTRUCTION.—Nothing in this subchapter shall be construed to alter or amend any law regarding the authority of any head of an agency over such agency.

''§ 3554. Agency responsibilities

''(a) IN GENERAL.—The head of each agency shall—

''(1) be responsible for—

''(A) complying with the policies and directives issued under section 3553;

''(B) providing information security protections commensurate with the risk resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by the agency or by a contractor of an agency or other organization on behalf of an agency; and

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(C) complying with the requirements of this subchapter, including—

''(i) information security standards and guidelines promulgated under section 11331 of title 40;

''(ii) for any national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued as directed by the President; and

''(iii) for any non-national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued under section 3553;

''(D) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

''(E) reporting and sharing, for an agency operating or exercising control of a national security system, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for national security systems issued as directed by the President; and

''(F) reporting and sharing, for those agencies operating or exercising control of non-national security systems, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for non-national security systems as prescribed under section 3553(a), including information to assist the entity designated under section 3555(a) with the ongoing security analysis under section 3555;

''(2) ensure that each senior agency official provides information security for the information and information systems that support the operations and assets under the senior agency official's control, including by—

''(A) assessing the risk and impact that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

''(B) determining the level of information security appropriate to protect such information and information systems in accordance with policies and directives issued under section 3553(a), and standards and guidelines promulgated under section 11331 of title 40 for information security classifications and related requirements;

''(C) implementing policies, procedures, and capabilities to reduce risks to an acceptable level in a cost-effective manner;

''(D) actively monitoring the effective implementation of information security controls and techniques; and

''(E) reporting information about information security incidents, cyber threat information, and deterioration of security controls in a timely and adequate manner to the entity designated under section 3553(a)(3) in accordance with paragraph (1);

''(3) assess and maintain the resiliency of information technology systems critical to agency mission and operations;

''(4) designate the agency Inspector General (or an independent entity selected in consultation with the Director and the Council of Inspectors General on Integrity and Efficiency if the agency does not have an Inspector General) to conduct the annual independent evaluation required under section 3556, and allow the agency Inspector General to contract with an independent entity to perform such evaluation;

''(5) delegate to the Chief Information Officer or equivalent (or to a senior agency official who reports to the Chief Information Officer or equivalent)—

''(A) the authority and primary responsibility to implement an agencywide information security program; and

''(B) the authority to provide information security for the information collected and maintained by the agency (or by a contractor, other agency, or other source on behalf of the agency) and for the information systems that support the operations, assets, and mission of the agency (including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency);

''(6) delegate to the appropriate agency official (who is responsible for a particular agency system or subsystem) the responsibility to ensure and enforce compliance with all requirements of the agency's agencywide information security program in coordination with the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5);

''(7) ensure that an agency has trained personnel who have obtained any necessary security clearances to permit them to assist the agency in complying with this subchapter;

''(8) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5), in coordination with other senior agency officials, reports to the agency head on the effectiveness of the agencywide information security program, including the progress of any remedial actions; and

''(9) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5) has the necessary qualifications to administer the functions described in this subchapter and has information security duties as a primary duty of that official.

''(b) CHIEF INFORMATION OFFICERS.—Each Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under subsection (a)(5) shall—

''(1) establish and maintain an enterprise security operations capability that on a continuous basis—

''(A) detects, reports, contains, mitigates, and responds to information security incidents that impair adequate security of the agency's information or information system in a timely manner and in accordance with the policies and directives under section 3553; and

''(B) reports any information security incident under subparagraph (A) to the entity designated under section 3555;

''(2) develop, maintain, and oversee an agencywide information security program;

''(3) develop, maintain, and oversee information security policies, procedures, and control techniques to address applicable requirements, including requirements under section 3553 of this title and section 11331 of title 40; and

''(4) train and oversee the agency personnel who have significant responsibility for information security with respect to that responsibility.

''(c) AGENCYWIDE INFORMATION SECURITY PROGRAMS.—

''(1) IN GENERAL.—Each agencywide information security program under subsection (b)(2) shall include—

''(A) relevant security risk assessments, including technical assessments and others related to the acquisition process;

''(B) security testing commensurate with risk and impact;

''(C) mitigation of deterioration of security controls commensurate with risk and impact;

''(D) risk-based continuous monitoring and threat assessment of the operational status and security of agency information systems to enable evaluation of the effectiveness of and compliance with information security policies, procedures, and practices, including a relevant and appropriate selection of security controls of information systems identified in the inventory under section 3505(c);

''(E) operation of appropriate technical capabilities in order to detect, mitigate, report, and respond to information security incidents, cyber threat information, and deterioration of security controls in a manner that is consistent with the policies and directives under section 3553, including—

''(i) mitigating risks associated with such information security incidents;

''(ii) notifying and consulting with the entity designated under section 3555; and

''(iii) notifying and consulting with, as appropriate—

''(I) law enforcement and the relevant Office of the Inspector General; and

''(II) any other entity, in accordance with law and as directed by the President;

''(F) a process to ensure that remedial action is taken to address any deficiencies in the information security policies, procedures, and practices of the agency; and

''(G) a plan and procedures to ensure the continuity of operations for information systems that support the operations and assets of the agency.

''(2) RISK MANAGEMENT STRATEGIES.—Each agencywide information security program under subsection (b)(2) shall include the development and maintenance of a risk management strategy for information security. The risk management strategy shall include—

''(A) consideration of information security incidents, cyber threat information, and deterioration of security controls; and

''(B) consideration of the consequences that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency;

''(3) POLICIES AND PROCEDURES.—Each agencywide information security program under subsection (b)(2) shall include policies and procedures that—

''(A) are based on the risk management strategy under paragraph (2);

''(B) reduce information security risks to an acceptable level in a cost-effective manner;

''(C) ensure that cost-effective and adequate information security is addressed as part of the acquisition and ongoing management of each agency information system; and

''(D) ensure compliance with—

''(i) this subchapter; and

''(ii) any other applicable requirements.

''(4) TRAINING REQUIREMENTS.—Each agencywide information security program under subsection (b)(2) shall include information security, privacy, civil rights, civil liberties, and information oversight training that meets any applicable requirements under section 3553. The training shall inform each information security personnel that has access to agency information systems (including contractors and other users of information systems that support the operations and assets of the agency) of—

''(A) the information security risks associated with the information security personnel's activities; and

''(B) the individual's responsibility to comply with the agency policies and procedures that reduce the risks under subparagraph (A).

''(d) ANNUAL REPORT.—Each agency shall submit a report annually to the Secretary of Homeland Security on its agencywide information security program and information systems.

''§ 3555. Multiagency ongoing threat assessment

''(a) IMPLEMENTATION.—The Director of the Office of Management and Budget, in coordination with the Secretary of Homeland Security, shall designate an entity to implement ongoing security analysis concerning agency information systems—

''(1) based on cyber threat information;

''(2) based on agency information system and environment of operation changes, including—

''(A) an ongoing evaluation of the information system security controls; and

''(B) the security state, risk level, and environment of operation of an agency information system, including—

''(i) a change in risk level due to a new cyber threat;

''(ii) a change resulting from a new technology;

''(iii) a change resulting from the agency's mission; and

''(iv) a change resulting from the business practice; and

''(3) using automated processes to the maximum extent possible—

''(A) to increase information system security;

''(B) to reduce paper-based reporting requirements; and

''(C) to maintain timely and actionable knowledge of the state of the information system security.

''(b) STANDARDS.—The National Institute of Standards and Technology may promulgate standards, in coordination with the Secretary of Homeland Security, to assist an agency with its duties under this section.

''(c) COMPLIANCE.—The head of each appropriate department and agency shall be responsible for ensuring compliance and implementing necessary procedures to comply with this section. The head of each appropriate department and agency, in consultation with the Director of the Office of Management and Budget and the Secretary of Homeland Security, shall—

''(1) monitor compliance under this section;

''(2) develop a timeline and implement for the department or agency—

''(A) adoption of any technology, system, or method that facilitates continuous monitoring and threat assessments of an agency information system;

''(B) adoption or updating of any technology, system, or method that prevents, detects, or remediates a significant cyber incident to a Federal information system of the department or agency that has impeded, or is reasonably likely to impede, the performance of a critical mission of the department or agency; and

''(C) adoption of any technology, system, or method that satisfies a requirement under this section.

''(d) LIMITATION OF AUTHORITY.—The authorities of the Director of the Office of Management and Budget and of the Secretary of Homeland Security under this section shall not apply to national security systems.

''(e) REPORT.—Not later than 6 months after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Government Accountability Office shall issue a report evaluating each agency's status toward implementing this section.

''§ 3556. Independent evaluations

''(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency, in consultation with the Director and the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense, shall issue and maintain criteria for the timely, cost-effective, risk-based, and independent evaluation of each agencywide information security program (and practices) to determine the effectiveness of the agencywide information security program (and practices). The criteria shall include measures to assess any conflicts of interest in the performance of the evaluation and whether the agencywide information security program includes appropriate safeguards against disclosure of information where such disclosure may adversely affect information security.

''(b) ANNUAL INDEPENDENT EVALUATIONS.—Each agency shall perform an annual independent evaluation of its agencywide information security program (and practices) in accordance with the criteria under subsection (a).

''(c) DISTRIBUTION OF REPORTS.—Not later than 30 days after receiving an independent evaluation under subsection (b), each agency head shall transmit a copy of the independent evaluation to the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense.

''(d) NATIONAL SECURITY SYSTEMS.—Evaluations involving national security systems shall be conducted as directed by President.

''§ 3557. National security systems.

''The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

''(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system; and

''(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President.''.

(b) SAVINGS PROVISIONS.—

(1) POLICY AND COMPLIANCE GUIDANCE.—Policy and compliance guidance issued by the Director before the date of enactment of this Act under section 3543(a)(1) of title 44, United States Code (as in effect on the day before the date of enactment of this Act), shall continue in effect, according to its terms, until modified, terminated, superseded, or repealed pursuant to section 3553(a)(1) of title 44, United States Code.

(2) STANDARDS AND GUIDELINES.—Standards and guidelines issued by the Secretary of Commerce or by the Director before the date of enactment of this Act under section 11331(a)(1) of title 40, United States Code, (as in effect on the day before the date of enactment of this Act) shall continue in effect, according to their terms, until modified, terminated, superseded, or repealed pursuant to section 11331(a)(1) of title 40, United States Code, as amended by this Act.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) CHAPTER ANALYSIS.—The chapter analysis for chapter 35 of title 44, United States Code, is amended—

(A) by striking the items relating to sections 3531 through 3538;

(B) by striking the items relating to sections 3541 through 3549; and

(C) by inserting the following:

''3551. Purposes.
''3552. Definitions.
''3553. Federal information security authority and coordination.
''3554. Agency responsibilities.
''3555. Multiagency ongoing threat assessment.
''3556. Independent evaluations.
''3557. National security systems.''.

(2) OTHER REFERENCES.—

(A) Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(1)(A)) is amended by striking ''section 3532(3)'' and inserting ''section 3552''.

(B) Section 2222(j)(5) of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(C) Section 2223(c)(3) of title 10, United States Code, is amended, by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(D) Section 2315 of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(E) Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended—

(i) in subsection (a)(2), by striking ''section 3532(b)(2)'' and inserting ''section 3552'';

(ii) in subsection (c)(3), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iii) in subsection (d)(1), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iv) in subsection (d)(8) by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(v) in subsection (d)(8), by striking ''submitted to the Director'' and inserting ''submitted to the Secretary'';

(vi) in subsection (e)(2), by striking ''section 3532(1) of such title'' and inserting ''section 3552 of title 44''; and

(vii) in subsection (e)(5), by striking ''section 3532(b)(2) of such title'' and inserting ''section 3552 of title 44''.

(F) Section 8(d)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7406(d)(1)) is amended by striking ''section 3534(b)'' and inserting ''section 3554(b)(2)''.

SEC. 202. MANAGEMENT OF INFORMATION TECHNOLOGY.

(a) IN GENERAL.—Section 11331 of title 40, United States Code, is amended to read as follows:

''§ 11331. Responsibilities for Federal information systems standards

''(a) STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO PRESCRIBE.—Except as provided under paragraph (2), the Secretary of Commerce shall prescribe standards and guidelines pertaining to Federal information systems—

''(A) in consultation with the Secretary of Homeland Security; and

''(B) on the basis of standards and guidelines developed by the National Institute of Standards and Technology under paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)(2) and (a)(3)).

''(2) NATIONAL SECURITY SYSTEMS.—Standards and guidelines for national security systems shall be developed, prescribed, enforced, and overseen as otherwise authorized by law and as directed by the President.

''(b) MANDATORY STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO MAKE MANDATORY STANDARDS AND GUIDELINES.—The Secretary of Commerce shall make standards and guidelines under subsection (a)(1) compulsory and binding to the extent determined necessary by the Secretary of Commerce to improve the efficiency of operation or security of Federal information systems.

''(2) REQUIRED MANDATORY STANDARDS AND GUIDELINES.—

''(A) IN GENERAL.—Standards and guidelines under subsection (a)(1) shall include information security standards that—

''(i) provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)); and

''(ii) are otherwise necessary to improve the security of Federal information and information systems.

''(B) BINDING EFFECT.—Information security standards under subparagraph (A) shall be compulsory and binding.

''(c) EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary of Commerce shall exercise the authority conferred by this section subject to direction by the President and in coordination with the Director.

''(d) APPLICATION OF MORE STRINGENT STANDARDS AND GUIDELINES.—The head of an executive agency may employ standards for the cost-effective information security for information systems within or under the supervision of that agency that are more stringent than the standards and guidelines the Secretary of Commerce prescribes under this section if the more stringent standards and guidelines—

''(1) contain at least the applicable standards and guidelines made compulsory and binding by the Secretary of Commerce; and

''(2) are otherwise consistent with the policies, directives, and implementation memoranda issued under section 3553(a) of title 44.

''(e) DECISIONS ON PROMULGATION OF STANDARDS AND GUIDELINES.—The decision by the Secretary of Commerce regarding the promulgation of any standard or guideline under this section shall occur not later than 6 months after the date of submission of the proposed standard to the Secretary of Commerce by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

''(f) NOTICE AND COMMENT.—A decision by the Secretary of Commerce to significantly modify, or not promulgate, a proposed standard submitted to the Secretary by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) shall be made after the public is given an opportunity to comment on the Secretary's proposed decision.

''(g) DEFINITIONS.—In this section:

''(1) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' has the meaning given the term in section 3552 of title 44.

''(2) INFORMATION SECURITY.—The term 'information security' has the meaning given the term in section 3552 of title 44.

''(3) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given the term in section 3552 of title 44.''.

SEC. 203. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 204. TECHNICAL AND CONFORMING AMENDMENTS.

Section 21(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4(b)) is amended—

(1) in paragraph (2), by striking ''and the Director of the Office of Management and Budget'' and inserting '', the Secretary of Commerce, and the Secretary of Homeland Security''; and

(2) in paragraph (3), by inserting '', the Secretary of Homeland Security,'' after ''the Secretary of Commerce''.

SEC. 205. CLARIFICATION OF AUTHORITIES.

Nothing in this title shall be construed to convey any new regulatory authority to any government entity implementing or complying with any provision of this title.

TITLE III—CRIMINAL PENALTIES

SEC. 301. PENALTIES FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030(c) of title 18, United States Code, is amended to read as follows:

''(c) The punishment for an offense under subsection (a) or (b) of this section is—

''(1) a fine under this title or imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(1) of this section;

''(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than 3 years, or both, in the case of an offense under subsection (a)(2); or

''(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2) of this section, if—

''(i) the offense was committed for purposes of commercial advantage or private financial gain;

''(ii) the offense was committed in the furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States, or of any State; or

''(iii) the value of the information obtained, or that would have been obtained if the offense was completed, exceeds $5,000;

''(3) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(3) of this section;

''(4) a fine under this title or imprisonment of not more than 20 years, or both, in the case of an offense under subsection (a)(4) of this section;

''(5)(A) except as provided in subparagraph (C), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A) of this section, if the offense caused—

''(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

''(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

''(iii) physical injury to any person;

''(iv) a threat to public health or safety;

''(v) damage affecting a computer used by, or on behalf of, an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

''(vi) damage affecting 10 or more protected computers during any 1-year period;

''(B) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(B), if the offense caused a harm provided in clause (i) through (vi) of subparagraph (A) of this subsection;

''(C) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both;

''(D) a fine under this title, imprisonment for not more than 10 years, or both, for any other offense under subsection (a)(5);

''(E) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(6) of this section; or

''(F) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(7) of this section.''.

SEC. 302. TRAFFICKING IN PASSWORDS.

Section 1030(a)(6) of title 18, United States Code, is amended to read as follows:

''(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information or means of access through which a protected computer (as defined in subparagraphs (A) and (B) of subsection (e)(2)) may be accessed without authorization.''.

SEC. 303. CONSPIRACY AND ATTEMPTED COMPUTER FRAUD OFFENSES.

Section 1030(b) of title 18, United States Code, is amended by inserting ''as if for the completed offense'' after ''punished as provided''.

SEC. 304. CRIMINAL AND CIVIL FORFEITURE FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030 of title 18, United States Code, is amended by striking subsections (i) and (j) and inserting the following:

''(i) CRIMINAL FORFEITURE.—

''(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

''(A) such persons interest in any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of such violation; and

''(B) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of such violation.

''(2) The criminal forfeiture of property under this subsection, including any seizure and disposition of the property, and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

''(j) CIVIL FORFEITURE.—

''(1) The following shall be subject to forfeiture to the United States and no property right, real or personal, shall exist in them:

''(A) Any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of any violation of this section, or a conspiracy to violate this section.

''(B) Any property, real or personal, constituting or derived from any gross proceeds obtained directly or indirectly, or any property traceable to such property, as a result of the commission of any violation of this section, or a conspiracy to violate this section.

''(2) Seizures and forfeitures under this subsection shall be governed by the provisions in chapter 46 relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents and other persons as may be designated for that purpose by the Secretary of Homeland Security or the Attorney General.''.

SEC. 305. DAMAGE TO CRITICAL INFRASTRUCTURE COMPUTERS.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

''§ 1030A. Aggravated damage to a critical infrastructure computer

''(a) DEFINITIONS.—In this section—

''(1) the term 'computer' has the meaning given the term in section 1030;

''(2) the term 'critical infrastructure computer' means a computer that manages or controls systems or assets vital to national defense, national security, national economic security, public health or safety, or any combination of those matters, whether publicly or privately owned or operated, including—

''(A) oil and gas production, storage, conversion, and delivery systems;

''(B) water supply systems;

''(C) telecommunication networks;

''(D) electrical power generation and delivery systems;

''(E) finance and banking systems;

''(F) emergency services;

''(G) transportation systems and services; and

''(H) government operations that provide essential services to the public; and

''(3) the term 'damage' has the meaning given the term in section 1030.

''(b) OFFENSE.—It shall be unlawful, during and in relation to a felony violation of section 1030, to knowingly cause or attempt to cause damage to a critical infrastructure computer if the damage results in (or, in the case of an attempt, if completed, would have resulted in) the substantial impairment—

''(1) of the operation of the critical infrastructure computer; or

''(2) of the critical infrastructure associated with the computer.

''(c) PENALTY.—Any person who violates subsection (b) shall be—

''(1) fined under this title;

''(2) imprisoned for not less than 3 years but not more than 20 years; or

''(3) penalized under paragraphs (1) and (2).

''(d) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

''(1) a court shall not place on probation any person convicted of a violation of this section;

''(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment, including any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for a felony violation of section 1030;

''(3) in determining any term of imprisonment to be imposed for a felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The chapter analysis for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

''1030A. Aggravated damage to a critical infrastructure computer.''.

SEC. 306. LIMITATION ON ACTIONS INVOLVING UNAUTHORIZED USE.

Section 1030(e)(6) of title 18, United States Code, is amended by striking ''alter;'' and inserting ''alter, but does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized;''.

SEC. 307. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

TITLE IV—CYBERSECURITY RESEARCH AND DEVELOPMENT

SEC. 401. NATIONAL HIGH-PERFORMANCE COMPUTING PROGRAM PLANNING AND COORDINATION.

(a) GOALS AND PRIORITIES.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(d) GOALS AND PRIORITIES.—The goals and priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include—

''(1) encouraging and supporting mechanisms for interdisciplinary research and development in networking and information technology, including—

''(A) through collaborations across agencies;

''(B) through collaborations across Program Component Areas;

''(C) through collaborations with industry;

''(D) through collaborations with institutions of higher education;

''(E) through collaborations with Federal laboratories (as defined in section 4 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3703)); and

''(F) through collaborations with international organizations;

''(2) addressing national, multi-agency, multi-faceted challenges of national importance; and

''(3) fostering the transfer of research and development results into new technologies and applications for the benefit of society.''.

(b) DEVELOPMENT OF STRATEGIC PLAN.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(e) STRATEGIC PLAN.—

''(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the agencies under subsection (a)(3)(B), working through the National Science and Technology Council and with the assistance of the Office of Science and Technology Policy shall develop a 5-year strategic plan to guide the activities under subsection (a)(1).

''(2) CONTENTS.—The strategic plan shall specify—

''(A) the near-term objectives for the Program;

''(B) the long-term objectives for the Program;

''(C) the anticipated time frame for achieving the near-term objectives;

''(D) the metrics that will be used to assess any progress made toward achieving the near-term objectives and the long-term objectives; and

''(E) how the Program will achieve the goals and priorities under subsection (d).

''(3) IMPLEMENTATION ROADMAP.—

''(A) IN GENERAL.—The agencies under subsection (a)(3)(B) shall develop and annually update an implementation roadmap for the strategic plan.

''(B) REQUIREMENTS.—The information in the implementation roadmap shall be coordinated with the database under section 102(c) and the annual report under section 101(a)(3). The implementation roadmap shall—

''(i) specify the role of each Federal agency in carrying out or sponsoring research and development to meet the research objectives of the strategic plan, including a description of how progress toward the research objectives will be evaluated, with consideration of any relevant recommendations of the advisory committee;

''(ii) specify the funding allocated to each major research objective of the strategic plan and the source of funding by agency for the current fiscal year; and

''(iii) estimate the funding required for each major research objective of the strategic plan for the next 3 fiscal years.

''(4) RECOMMENDATIONS.—The agencies under subsection (a)(3)(B) shall take into consideration when developing the strategic plan under paragraph (1) the recommendations of—

''(A) the advisory committee under subsection (b); and

''(B) the stakeholders under section 102(a)(3).

''(5) REPORT TO CONGRESS.—The Director of the Office of Science and Technology Policy shall transmit the strategic plan under this subsection, including the implementation roadmap and any updates under paragraph (3), to—

''(A) the advisory committee under subsection (b);

''(B) the Committee on Commerce, Science, and Transportation of the Senate; and

''(C) the Committee on Science and Technology of the House of Representatives.''.

(c) PERIODIC REVIEWS.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(f) PERIODIC REVIEWS.—The agencies under subsection (a)(3)(B) shall—

''(1) periodically assess the contents and funding levels of the Program Component Areas and restructure the Program when warranted, taking into consideration any relevant recommendations of the advisory committee under subsection (b); and

''(2) ensure that the Program includes national, multi-agency, multi-faceted research and development activities, including activities described in section 104.''.

(d) ADDITIONAL RESPONSIBILITIES OF DIRECTOR.—Section 101(a)(2) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(2)) is amended—

(1) by redesignating subparagraphs (E) and (F) as subparagraphs (G) and (H), respectively; and

(2) by inserting after subparagraph (D) the following:

''(E) encourage and monitor the efforts of the agencies participating in the Program to allocate the level of resources and management attention necessary—

''(i) to ensure that the strategic plan under subsection (e) is developed and executed effectively; and

''(ii) to ensure that the objectives of the Program are met;

''(F) working with the Office of Management and Budget and in coordination with the creation of the database under section 102(c), direct the Office of Science and Technology Policy and the agencies participating in the Program to establish a mechanism (consistent with existing law) to track all ongoing and completed research and development projects and associated funding;''.

(e) ADVISORY COMMITTEE.—Section 101(b) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(b)) is amended—

(1) in paragraph (1)—

(A) by inserting after the first sentence the following: ''The co-chairs of the advisory committee shall meet the qualifications of committee members and may be members of the Presidents Council of Advisors on Science and Technology.''; and

(B) by striking ''high-performance'' in subparagraph (D) and inserting ''high-end''; and

(2) by amending paragraph (2) to read as follows:

''(2) In addition to the duties under paragraph (1), the advisory committee shall conduct periodic evaluations of the funding, management, coordination, implementation, and activities of the Program. The advisory committee shall report its findings and recommendations not less frequently than once every 3 fiscal years to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives. The report shall be submitted in conjunction with the update of the strategic plan.''.

(f) REPORT.—Section 101(a)(3) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(3)) is amended—

(1) in subparagraph (C)—

(A) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(B) by striking ''each Program Component Area'' and inserting ''each Program Component Area and each research area supported in accordance with section 104'';

(2) in subparagraph (D)—

(A) by striking ''each Program Component Area,'' and inserting ''each Program Component Area and each research area supported in accordance with section 104,'';

(B) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(C) by striking ''and'' after the semicolon;

(3) by redesignating subparagraph (E) as subparagraph (G); and

(4) by inserting after subparagraph (D) the following:

''(E) include a description of how the objectives for each Program Component Area, and the objectives for activities that involve multiple Program Component Areas, relate to the objectives of the Program identified in the strategic plan under subsection (e);

''(F) include—

''(i) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the next fiscal year by category of activity;

''(ii) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the current fiscal year by category of activity; and

''(iii) the amount of funding provided for the Office of Science and Technology Policy for the current fiscal year by each agency participating in the Program; and''.

(g) DEFINITIONS.—Section 4 of the High-Performance Computing Act of 1991 (15 U.S.C. 5503) is amended—

(1) by redesignating paragraphs (1) and (2) as paragraphs (2) and (3), respectively;

(2) by redesignating paragraph (3) as paragraph (6);

(3) by redesignating paragraphs (6) and (7) as paragraphs (7) and (8), respectively;

(4) by inserting before paragraph (2), as redesignated, the following:

''(1) 'cyber-physical systems' means physical or engineered systems whose networking

and information technology functions and physical elements are deeply integrated and are actively connected to the physical world through sensors, actuators, or other means to perform monitoring and control functions;'';

(5) in paragraph (3), as redesignated, by striking ''high-performance computing'' and inserting ''networking and information technology'';

(6) in paragraph (6), as redesignated—

(A) by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(B) by striking ''supercomputer'' and inserting ''high-end computing'';

(7) in paragraph (5), by striking ''network referred to as'' and all that follows through the semicolon and inserting ''network, including advanced computer networks of Federal agencies and departments''; and

(8) in paragraph (7), as redesignated, by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program''.

SEC. 402. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

(a) RESEARCH IN AREAS OF NATIONAL IMPORTANCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.) is amended by adding at the end the following:

''SEC. 104. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

''(a) IN GENERAL.—The Program shall encourage agencies under section 101(a)(3)(B) to support, maintain, and improve national, multi-agency, multi-faceted, research and development activities in networking and information technology directed toward application areas that have the potential for significant contributions to national economic competitiveness and for other significant societal benefits.

''(b) TECHNICAL SOLUTIONS.—An activity under subsection (a) shall be designed to advance the development of research discoveries by demonstrating technical solutions to important problems in areas including—

''(1) cybersecurity;

''(2) health care;

''(3) energy management and low-power systems and devices;

''(4) transportation, including surface and air transportation;

''(5) cyber-physical systems;

''(6) large-scale data analysis and modeling of physical phenomena;

''(7) large scale data analysis and modeling of behavioral phenomena;

''(8) supply chain quality and security; and

''(9) privacy protection and protected disclosure of confidential data.

''(c) RECOMMENDATIONS.—The advisory committee under section 101(b) shall make recommendations to the Program for candidate research and development areas for support under this section.

''(d) CHARACTERISTICS.—

''(1) IN GENERAL.—Research and development activities under this section—

''(A) shall include projects selected on the basis of applications for support through a competitive, merit-based process;

''(B) shall leverage, when possible, Federal investments through collaboration with related State initiatives;

''(C) shall include a plan for fostering the transfer of research discoveries and the results of technology demonstration activities, including from institutions of higher education and Federal laboratories, to industry for commercial development;

''(D) shall involve collaborations among researchers in institutions of higher education and industry; and

''(E) may involve collaborations among nonprofit research institutions and Federal laboratories, as appropriate.

''(2) COST-SHARING.—In selecting applications for support, the agencies under section 101(a)(3)(B) shall give special consideration to projects that include cost sharing from non-Federal sources.

''(3) MULTIDISCIPLINARY RESEARCH CENTERS.—Research and development activities under this section shall be supported through multidisciplinary research centers, including Federal laboratories, that are organized to investigate basic research questions and carry out technology demonstration activities in areas described in subsection (a). Research may be carried out through existing multidisciplinary centers, including those authorized under section 7024(b)(2) of the America COMPETES Act (42 U.S.C. 1862o–10(2)).''.

(b) CYBER-PHYSICAL SYSTEMS.—Section 101(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following:

''(J) provide for increased understanding of the scientific principles of cyber-physical systems and improve the methods available for the design, development, and operation of cyber-physical systems that are characterized by high reliability, safety, and security; and

''(K) provide for research and development on human-computer interactions, visualization, and big data.''.

(c) TASK FORCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.), as amended by section 402(a) of this Act, is amended by adding at the end the following:

''SEC. 105. TASK FORCE.

''(a) ESTABLISHMENT.—Not later than 180 days after the date of enactment the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy under section 102 shall convene a task force to explore mechanisms for carrying out collaborative research and development activities for cyber-physical systems (including the related technologies required to enable these systems) through a consortium or other appropriate entity with participants from institutions of higher education, Federal laboratories, and industry.

''(b) FUNCTIONS.—The task force shall—

''(1) develop options for a collaborative model and an organizational structure for such entity under which the joint research and development activities could be planned, managed, and conducted effectively, including mechanisms for the allocation of resources among the participants in such entity for support of such activities;

''(2) propose a process for developing a research and development agenda for such entity, including guidelines to ensure an appropriate scope of work focused on nationally significant challenges and requiring collaboration and to ensure the development of related scientific and technological milestones;

''(3) define the roles and responsibilities for the participants from institutions of higher education, Federal laboratories, and industry in such entity;

''(4) propose guidelines for assigning intellectual property rights and for transferring research results to the private sector; and

''(5) make recommendations for how such entity could be funded from Federal, State, and non-governmental sources.

''(c) COMPOSITION.—In establishing the task force under subsection (a), the Director of the Office of Science and Technology Policy shall appoint an equal number of individuals from institutions of higher education and from industry with knowledge and expertise in cyber-physical systems, and may appoint not more than 2 individuals from Federal laboratories.

''(d) REPORT.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy shall transmit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives a report describing the findings and recommendations of the task force.

''(e) TERMINATION.—The task force shall terminate upon transmittal of the report required under subsection (d).

''(f) COMPENSATION AND EXPENSES.—Members of the task force shall serve without compensation.''.

SEC. 403. PROGRAM IMPROVEMENTS.

Section 102 of the High-Performance Computing Act of 1991 (15 U.S.C. 5512) is amended to read as follows:

''SEC. 102. PROGRAM IMPROVEMENTS.

''(a) FUNCTIONS.—The Director of the Office of Science and Technology Policy shall continue—

''(1) to provide technical and administrative support to—

''(A) the agencies participating in planning and implementing the Program, including support needed to develop the strategic plan under section 101(e); and

''(B) the advisory committee under section 101(b);

''(2) to serve as the primary point of contact on Federal networking and information technology activities for government agencies, academia, industry, professional societies, State computing and networking technology programs, interested citizen groups, and others to exchange technical and programmatic information;

''(3) to solicit input and recommendations from a wide range of stakeholders during the development of each strategic plan under section 101(e) by convening at least 1 workshop with invitees from academia, industry, Federal laboratories, and other relevant organizations and institutions;

''(4) to conduct public outreach, including the dissemination of the advisory committee's findings and recommendations, as appropriate;

''(5) to promote access to and early application of the technologies, innovations, and expertise derived from Program activities to agency missions and systems across the Federal Government and to United States industry;

''(6) to ensure accurate and detailed budget reporting of networking and information technology research and development investment; and

''(7) to encourage agencies participating in the Program to use existing programs and resources to strengthen networking and information technology education and training, and increase participation in such fields, including by women and underrepresented minorities.

''(b) SOURCE OF FUNDING.—

''(1) IN GENERAL.—The functions under this section shall be supported by funds from each agency participating in the Program.

''(2) SPECIFICATIONS.—The portion of the total budget of the Office of Science and Technology Policy that is provided by each agency participating in the Program for each

fiscal year shall be in the same proportion as each agency's share of the total budget for the Program for the previous fiscal year, as specified in the database under section 102(c).

''(c) DATABASE.—

''(1) IN GENERAL.—The Director of the Office of Science and Technology Policy shall develop and maintain a database of projects funded by each agency for the fiscal year for each Program Component Area.

''(2) PUBLIC ACCESSIBILITY.—The Director of the Office of Science and Technology Policy shall make the database accessible to the public.

''(3) DATABASE CONTENTS.—The database shall include, for each project in the database—

''(A) a description of the project;

''(B) each agency, industry, institution of higher education, Federal laboratory, or international institution involved in the project;

''(C) the source funding of the project (set forth by agency);

''(D) the funding history of the project; and

''(E) whether the project has been completed.''.

SEC. 404. IMPROVING EDUCATION OF NETWORKING AND INFORMATION TECHNOLOGY, INCLUDING HIGH PERFORMANCE COMPUTING.

Section 201(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)) is amended—

(1) by redesignating paragraphs (2) through (4) as paragraphs (3) through (5), respectively; and

(2) by inserting after paragraph (1) the following:

''(2) the National Science Foundation shall use its existing programs, in collaboration with other agencies, as appropriate, to improve the teaching and learning of networking and information technology at all levels of education and to increase participation in networking and information technology fields;''.

SEC. 405. CONFORMING AND TECHNICAL AMENDMENTS TO THE HIGH-PERFORMANCE COMPUTING ACT OF 1991.

(a) SECTION 3.—Section 3 of the High-Performance Computing Act of 1991 (15 U.S.C. 5502) is amended—

(1) in the matter preceding paragraph (1), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(2) in paragraph (1)—

(A) in the matter preceding subparagraph (A), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(B) in subparagraphs (A), (F), and (G), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(C) in subparagraph (H), by striking ''high-performance'' and inserting ''high-end''; and

(3) in paragraph (2)—

(A) by striking ''high-performance computing and'' and inserting ''networking and information technology, and''; and

(B) by striking ''high-performance computing network'' and inserting ''networking and information technology''.

(b) TITLE HEADING.—The heading of title I of the High-Performance Computing Act of 1991 (105 Stat. 1595) is amended by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''.

(c) SECTION 101.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT**'';

(2) in subsection (a)—

(A) in the subsection heading, by striking ''NATIONAL HIGH-PERFORMANCE COMPUTING'' and inserting ''NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT'';

(B) in paragraph (1)—

(i) by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program'';

(ii) in subparagraph (A), by striking ''high-performance computing, including networking'' and inserting ''networking and information technology'';

(iii) in subparagraphs (B) and (G), by striking ''high-performance'' each place it appears and inserting ''high-end''; and

(iv) in subparagraph (C), by striking ''high-performance computing and networking'' and inserting ''high-end computing, distributed, and networking''; and

(C) in paragraph (2)—

(i) in subparagraphs (A) and (C)—

(I) by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(II) by striking ''development, networking,'' each place it appears and inserting ''development,''; and

(ii) in subparagraphs (G) and (H), as redesignated by section 401(d) of this Act, by striking ''high-performance'' each place it appears and inserting ''high-end'';

(3) in subsection (b)(1), in the matter preceding subparagraph (A), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(4) in subsection (c)(1)(A), by striking ''high-performance computing'' and inserting ''networking and information technology''.

(d) SECTION 201.—Section 201(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)(1)) is amended by striking ''high-performance computing and advanced high-speed computer networking'' and inserting ''networking and information technology research and development''.

(e) SECTION 202.—Section 202(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5522(a)) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(f) SECTION 203.—Section 203(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5523(a)) is amended—

(1) in paragraph (1), by striking ''high-performance computing and networking'' and inserting ''networking and information technology''; and

(2) in paragraph (2)(A), by striking ''high-performance'' and inserting ''high-end''.

(g) SECTION 204.—Section 204 of the High-Performance Computing Act of 1991 (15 U.S.C. 5524) is amended—

(1) in subsection (a)(1)—

(A) in subparagraph (A), by striking ''high-performance computing systems and networks'' and inserting ''networking and information technology systems and capabilities'';

(B) in subparagraph (B), by striking ''interoperability of high-performance computing systems in networks and for common user interfaces to systems'' and inserting ''interoperability and usability of networking and information technology systems''; and

(C) in subparagraph (C), by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(2) in subsection (b)—

(A) by striking ''HIGH-PERFORMANCE COMPUTING AND NETWORK'' in the heading and inserting ''NETWORKING AND INFORMATION TECHNOLOGY''; and

(B) by striking ''sensitive''.

(h) SECTION 205.—Section 205(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5525(a)) is amended by striking ''computational'' and inserting ''networking and information technology''.

(i) SECTION 206.—Section 206(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5526(a)) is amended by striking ''computational research'' and inserting ''networking and information technology research''.

(j) SECTION 207.—Section 207 of the High-Performance Computing Act of 1991 (15 U.S.C. 5527) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(k) SECTION 208.—Section 208 of the High-Performance Computing Act of 1991 (15 U.S.C. 5528) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''; and

(2) in subsection (a)—

(A) in paragraph (1), by striking ''High-performance computing and associated'' and inserting ''Networking and information'';

(B) in paragraph (2), by striking ''high-performance computing'' and inserting ''networking and information technologies'';

(C) in paragraph (3), by striking ''high-performance'' and inserting ''high-end'';

(D) in paragraph (4), by striking ''high-performance computers and associated'' and inserting ''networking and information''; and

(E) in paragraph (5), by striking ''high-performance computing and associated'' and inserting ''networking and information''.

SEC. 406. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation, in coordination with the Secretary of Homeland Security, shall carry out a Federal cyber scholarship-for-service program to recruit and train the next generation of information technology professionals and security managers to meet the needs of the cybersecurity mission for the Federal government.

(b) PROGRAM DESCRIPTION AND COMPONENTS.—The program shall—

(1) annually assess the workforce needs of the Federal government for cybersecurity professionals, including network engineers, software engineers, and other experts in order to determine how many scholarships should be awarded annually to ensure that the workforce needs following graduation match the number of scholarships awarded;

(2) provide scholarships for up to 1,000 students per year in their pursuit of undergraduate or graduate degrees in the cybersecurity field, in an amount that may include coverage for full tuition, fees, and a stipend;

(3) require each scholarship recipient, as a condition of receiving a scholarship under the program, to serve in a Federal information technology workforce for a period equal to one and one-half times each year, or partial year, of scholarship received, in addition to an internship in the cybersecurity field, if applicable, following graduation;

(4) provide a procedure for the National Science Foundation or a Federal agency, consistent with regulations of the Office of Personnel Management, to request and fund a security clearance for a scholarship recipient, including providing for clearance during a summer internship and upon graduation; and

(5) provide opportunities for students to receive temporary appointments for meaningful employment in the Federal information technology workforce during school vacation periods and for internships.

(c) HIRING AUTHORITY.—

(1) IN GENERAL.—For purposes of any law or regulation governing the appointment of an

individual in the Federal civil service, upon the successful completion of the student's studies, a student receiving a scholarship under the program may—

(A) be hired under section 213.3102(r) of title 5, Code of Federal Regulations; and

(B) be exempt from competitive service.

(2) COMPETITIVE SERVICE.—Upon satisfactory fulfillment of the service term under paragraph (1), an individual may be converted to a competitive service position without competition if the individual meets the requirements for that position.

(d) ELIGIBILITY.—The eligibility requirements for a scholarship under this section shall include that a scholarship applicant—

(1) be a citizen of the United States;

(2) be eligible to be granted a security clearance;

(3) maintain a grade point average of 3.2 or above on a 4.0 scale for undergraduate study or a 3.5 or above on a 4.0 scale for postgraduate study;

(4) demonstrate a commitment to a career in improving the security of the information infrastructure; and

(5) has demonstrated a level of proficiency in math or computer sciences.

(e) FAILURE TO COMPLETE SERVICE OBLIGATION.—

(1) IN GENERAL.—A scholarship recipient under this section shall be liable to the United States under paragraph (2) if the scholarship recipient—

(A) fails to maintain an acceptable level of academic standing in the educational institution in which the individual is enrolled, as determined by the Director;

(B) is dismissed from such educational institution for disciplinary reasons;

(C) withdraws from the program for which the award was made before the completion of such program;

(D) declares that the individual does not intend to fulfill the service obligation under this section;

(E) fails to fulfill the service obligation of the individual under this section; or

(F) loses a security clearance or becomes ineligible for a security clearance.

(2) REPAYMENT AMOUNTS.—

(A) LESS THAN 1 YEAR OF SERVICE.—If a circumstance under paragraph (1) occurs before the completion of 1 year of a service obligation under this section, the total amount of awards received by the individual under this section shall be repaid.

(B) ONE OR MORE YEARS OF SERVICE.—If a circumstance described in subparagraph (D) or (E) of paragraph (1) occurs after the completion of 1 year of a service obligation under this section, the total amount of scholarship awards received by the individual under this section, reduced by the ratio of the number of years of service completed divided by the number of years of service required, shall be repaid.

(f) EVALUATION AND REPORT.—The Director of the National Science Foundation shall—

(1) evaluate the success of recruiting individuals for scholarships under this section and of hiring and retaining those individuals in the public sector workforce, including the annual cost and an assessment of how the program actually improves the Federal workforce; and

(2) periodically report the findings under paragraph (1) to Congress.

(g) AUTHORIZATION OF APPROPRIATIONS.—From amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), the Director may use funds to carry out the requirements of this section for fiscal years 2012 through 2013.

SEC. 407. STUDY AND ANALYSIS OF CERTIFICATION AND TRAINING OF INFORMATION INFRASTRUCTURE PROFESSIONALS.

(a) STUDY.—The President shall enter into an agreement with the National Academies to conduct a comprehensive study of government, academic, and private-sector accreditation, training, and certification programs for personnel working in information infrastructure. The agreement shall require the National Academies to consult with sector coordinating councils and relevant governmental agencies, regulatory entities, and nongovernmental organizations in the course of the study.

(b) SCOPE.—The study shall include—

(1) an evaluation of the body of knowledge and various skills that specific categories of personnel working in information infrastructure should possess in order to secure information systems;

(2) an assessment of whether existing government, academic, and private-sector accreditation, training, and certification programs provide the body of knowledge and various skills described in paragraph (1);

(3) an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity talent, including barriers relating to compensation, the hiring process, job classification, and hiring flexibility; and

(4) an analysis of the sources and availability of cybersecurity talent, a comparison of the skills and expertise sought by the Federal Government and the private sector, an examination of the current and future capacity of United States institutions of higher education, including community colleges, to provide current and future cybersecurity professionals, through education and training activities, with those skills sought by the Federal Government, State and local entities, and the private sector.

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the National Academies shall submit to the President and Congress a report on the results of the study. The report shall include—

(1) findings regarding the state of information infrastructure accreditation, training, and certification programs, including specific areas of deficiency and demonstrable progress; and

(2) recommendations for the improvement of information infrastructure accreditation, training, and certification programs.

SEC. 408. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

(a) IN GENERAL.—The Director of the National Institute of Standards and Technology, in coordination with appropriate Federal authorities, shall—

(1) as appropriate, ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to Congress a plan for ensuring such Federal agency coordination.

(b) CONSULTATION WITH THE PRIVATE SECTOR.—In carrying out the activities under subsection (a)(1), the Director shall ensure consultation with appropriate private sector stakeholders.

SEC. 409. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

The Director of the National Institute of Standards and Technology shall continue a program to support the development of technical standards, metrology, testbeds, and conformance criteria, taking into account appropriate user concerns—

(1) to improve interoperability among identity management technologies;

(2) to strengthen authentication methods of identity management systems;

(3) to improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols; and

(4) to improve the usability of identity management systems.

SEC. 410. FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY RESEARCH GRANT AREAS.—Section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking ''property.'' and inserting ''property;''; and

(3) by adding at the end the following:

''(J) secure fundamental protocols that are at the heart of inter-network communications and data exchange;

''(K) system security that addresses the building of secure systems from trusted and untrusted components;

''(L) monitoring and detection; and

''(M) resiliency and rapid recovery methods.''.

(b) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY GRANTS.—Section 4(a)(3) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(3)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(c) COMPUTER AND NETWORK SECURITY CENTERS.—Section 4(b)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7403(b)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(d) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—Section 5(a)(6) of the Cyber Security Research and Development Act (15 U.S.C. 7404(a)(6)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT GRANTS.—Section 5(b)(2) of the Cyber Security Research and Development Act (15 U.S.C. 7404(b)(2)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(f) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY RESEARCH.—Section 5(c)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7404(c)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

SA 2609. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. LIMITATION ON FOREIGN ASSISTANCE TO PAKISTAN.

No amounts may be obligated or expended to provide any direct United States assistance to the Government of Pakistan unless the President certifies to Congress that—

(1) Dr. Shakil Afridi has been released from prison in Pakistan;

(2) any criminal charges brought against Dr. Afridi, including treason, have been dropped; and

(3) if necessary to ensure his freedom, Dr. Afridi has been allowed to leave Pakistan.

SA 2610. Mrs. HUTCHISON submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 106, strike line 8 and all that follows through page 156, line 13, and insert the following:

TITLE III—CYBERSECURITY RESEARCH AND DEVELOPMENT

SEC. 301. NATIONAL HIGH-PERFORMANCE COMPUTING PROGRAM PLANNING AND COORDINATION.

(a) GOALS AND PRIORITIES.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(d) GOALS AND PRIORITIES.—The goals and priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include—

''(1) encouraging and supporting mechanisms for interdisciplinary research and development in networking and information technology, including—

''(A) through collaborations across agencies;

''(B) through collaborations across Program Component Areas;

''(C) through collaborations with industry;

''(D) through collaborations with institutions of higher education;

''(E) through collaborations with Federal laboratories (as defined in section 4 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3703)); and

''(F) through collaborations with international organizations;

''(2) addressing national, multi-agency, multi-faceted challenges of national importance; and

''(3) fostering the transfer of research and development results into new technologies and applications for the benefit of society.''.

(b) DEVELOPMENT OF STRATEGIC PLAN.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(e) STRATEGIC PLAN.—

''(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Cybersecurity Act of 2012, the agencies under subsection (a)(3)(B), working through the National Science and Technology Council and with the assistance of the Office of Science and Technology Policy shall develop a 5-year strategic plan to guide the activities under subsection (a)(1).

''(2) CONTENTS.—The strategic plan shall specify—

''(A) the near-term objectives for the Program;

''(B) the long-term objectives for the Program;

''(C) the anticipated time frame for achieving the near-term objectives;

''(D) the metrics that will be used to assess any progress made toward achieving the near-term objectives and the long-term objectives; and

''(E) how the Program will achieve the goals and priorities under subsection (d).

''(3) IMPLEMENTATION ROADMAP.—

''(A) IN GENERAL.—The agencies under subsection (a)(3)(B) shall develop and annually update an implementation roadmap for the strategic plan.

''(B) REQUIREMENTS.—The information in the implementation roadmap shall be coordinated with the database under section 102(c) and the annual report under section 101(a)(3). The implementation roadmap shall—

''(i) specify the role of each Federal agency in carrying out or sponsoring research and development to meet the research objectives of the strategic plan, including a description of how progress toward the research objectives will be evaluated, with consideration of any relevant recommendations of the advisory committee;

''(ii) specify the funding allocated to each major research objective of the strategic plan and the source of funding by agency for the current fiscal year; and

''(iii) estimate the funding required for each major research objective of the strategic plan for the next 3 fiscal years.

''(4) RECOMMENDATIONS.—The agencies under subsection (a)(3)(B) shall take into consideration when developing the strategic plan under paragraph (1) the recommendations of—

''(A) the advisory committee under subsection (b); and

''(B) the stakeholders under section 102(a)(3).

''(5) REPORT TO CONGRESS.—The Director of the Office of Science and Technology Policy shall transmit the strategic plan under this subsection, including the implementation roadmap and any updates under paragraph (3), to—

''(A) the advisory committee under subsection (b);

''(B) the Committee on Commerce, Science, and Transportation of the Senate; and

''(C) the Committee on Science and Technology of the House of Representatives.''.

(c) PERIODIC REVIEWS.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(f) PERIODIC REVIEWS.—The agencies under subsection (a)(3)(B) shall—

''(1) periodically assess the contents and funding levels of the Program Component Areas and restructure the Program when warranted, taking into consideration any relevant recommendations of the advisory committee under subsection (b); and

''(2) ensure that the Program includes national, multi-agency, multi-faceted research and development activities, including activities described in section 104.''.

(d) ADDITIONAL RESPONSIBILITIES OF DIRECTOR.—Section 101(a)(2) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(2)) is amended—

(1) by redesignating subparagraphs (E) and (F) as subparagraphs (G) and (H), respectively; and

(2) by inserting after subparagraph (D) the following:

''(E) encourage and monitor the efforts of the agencies participating in the Program to allocate the level of resources and management attention necessary—

''(i) to ensure that the strategic plan under subsection (e) is developed and executed effectively; and

''(ii) to ensure that the objectives of the Program are met;

''(F) working with the Office of Management and Budget and in coordination with the creation of the database under section 102(c), direct the Office of Science and Technology Policy and the agencies participating in the Program to establish a mechanism (consistent with existing law) to track all ongoing and completed research and development projects and associated funding;''.

(e) ADVISORY COMMITTEE.—Section 101(b) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(b)) is amended—

(1) in paragraph (1)—

(A) by inserting after the first sentence the following: ''The co-chairs of the advisory committee shall meet the qualifications of committee members and may be members of the Presidents Council of Advisors on Science and Technology.''; and

(B) by striking ''high-performance'' in subparagraph (D) and inserting ''high-end''; and

(2) by amending paragraph (2) to read as follows:

''(2) In addition to the duties under paragraph (1), the advisory committee shall conduct periodic evaluations of the funding, management, coordination, implementation, and activities of the Program. The advisory committee shall report its findings and recommendations not less frequently than once every 3 fiscal years to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives. The report shall be submitted in conjunction with the update of the strategic plan.''.

(f) REPORT.—Section 101(a)(3) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(3)) is amended—

(1) in subparagraph (C)—

(A) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(B) by striking ''each Program Component Area'' and inserting ''each Program Component Area and each research area supported in accordance with section 104'';

(2) in subparagraph (D)—

(A) by striking ''each Program Component Area,'' and inserting ''each Program Component Area and each research area supported in accordance with section 104,'';

(B) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(C) by striking ''and'' after the semicolon;

(3) by redesignating subparagraph (E) as subparagraph (G); and

(4) by inserting after subparagraph (D) the following:

''(E) include a description of how the objectives for each Program Component Area, and the objectives for activities that involve multiple Program Component Areas, relate to the objectives of the Program identified in the strategic plan under subsection (e);

''(F) include—

''(i) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the next fiscal year by category of activity;

''(ii) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the current fiscal year by category of activity; and

''(iii) the amount of funding provided for the Office of Science and Technology Policy for the current fiscal year by each agency participating in the Program; and''.

(g) DEFINITIONS.—Section 4 of the High-Performance Computing Act of 1991 (15 U.S.C. 5503) is amended—

(1) by redesignating paragraphs (1) and (2) as paragraphs (2) and (3), respectively;

(2) by redesignating paragraph (3) as paragraph (6);

(3) by redesignating paragraphs (6) and (7) as paragraphs (7) and (8), respectively;

(4) by inserting before paragraph (2), as redesignated, the following:

''(1) 'cyber-physical systems' means physical or engineered systems whose networking and information technology functions and physical elements are deeply integrated and are actively connected to the physical world through sensors, actuators, or other means to perform monitoring and control functions;'';

(5) in paragraph (3), as redesignated, by striking ''high-performance computing'' and inserting ''networking and information technology'';

(6) in paragraph (6), as redesignated—

(A) by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(B) by striking ''supercomputer'' and inserting ''high-end computing'';

(7) in paragraph (5), by striking ''network referred to as'' and all that follows through the semicolon and inserting ''network, including advanced computer networks of Federal agencies and departments''; and

(8) in paragraph (7), as redesignated, by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program''.

SEC. 302. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

(a) RESEARCH IN AREAS OF NATIONAL IMPORTANCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.) is amended by adding at the end the following:

''SEC. 104. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

''(a) IN GENERAL.—The Program shall encourage agencies under section 101(a)(3)(B) to support, maintain, and improve national, multi-agency, multi-faceted, research and development activities in networking and information technology directed toward application areas that have the potential for significant contributions to national economic competitiveness and for other significant societal benefits.

''(b) TECHNICAL SOLUTIONS.—An activity under subsection (a) shall be designed to advance the development of research discoveries by demonstrating technical solutions to important problems in areas including—

''(1) cybersecurity;

''(2) health care;

''(3) energy management and low-power systems and devices;

''(4) transportation, including surface and air transportation;

''(5) cyber-physical systems;

''(6) large-scale data analysis and modeling of physical phenomena;

''(7) large scale data analysis and modeling of behavioral phenomena;

''(8) supply chain quality and security; and

''(9) privacy protection and protected disclosure of confidential data.

''(c) RECOMMENDATIONS.—The advisory committee under section 101(b) shall make recommendations to the Program for candidate research and development areas for support under this section.

''(d) CHARACTERISTICS.—

''(1) IN GENERAL.—Research and development activities under this section—

''(A) shall include projects selected on the basis of applications for support through a competitive, merit-based process;

''(B) shall leverage, when possible, Federal investments through collaboration with related State initiatives;

''(C) shall include a plan for fostering the transfer of research discoveries and the results of technology demonstration activities, including from institutions of higher education and Federal laboratories, to industry for commercial development;

''(D) shall involve collaborations among researchers in institutions of higher education and industry; and

''(E) may involve collaborations among nonprofit research institutions and Federal laboratories, as appropriate.

''(2) COST-SHARING.—In selecting applications for support, the agencies under section 101(a)(3)(B) shall give special consideration to projects that include cost sharing from non-Federal sources.

''(3) MULTIDISCIPLINARY RESEARCH CENTERS.—Research and development activities under this section shall be supported through multidisciplinary research centers, including Federal laboratories, that are organized to investigate basic research questions and carry out technology demonstration activities in areas described in subsection (a). Research may be carried out through existing multidisciplinary centers, including those authorized under section 7024(b)(2) of the America COMPETES Act (42 U.S.C. 1862o–10(2)).''.

(b) CYBER-PHYSICAL SYSTEMS.—Section 101(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following:

''(J) provide for increased understanding of the scientific principles of cyber-physical systems and improve the methods available for the design, development, and operation of cyber-physical systems that are characterized by high reliability, safety, and security; and

''(K) provide for research and development on human-computer interactions, visualization, and big data.''.

(c) TASK FORCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.), as amended by section 302(a) of this Act, is amended by adding at the end the following:

''SEC. 105. TASK FORCE.

''(a) ESTABLISHMENT.—Not later than 180 days after the date of enactment the Cybersecurity Act of 2012, the Director of the Office of Science and Technology Policy under section 102 shall convene a task force to explore mechanisms for carrying out collaborative research and development activities for cyber-physical systems (including the related technologies required to enable these systems) through a consortium or other appropriate entity with participants from institutions of higher education, Federal laboratories, and industry.

''(b) FUNCTIONS.—The task force shall—

''(1) develop options for a collaborative model and an organizational structure for such entity under which the joint research and development activities could be planned, managed, and conducted effectively, including mechanisms for the allocation of resources among the participants in such entity for support of such activities;

''(2) propose a process for developing a research and development agenda for such entity, including guidelines to ensure an appropriate scope of work focused on nationally significant challenges and requiring collaboration and to ensure the development of related scientific and technological milestones;

''(3) define the roles and responsibilities for the participants from institutions of higher education, Federal laboratories, and industry in such entity;

''(4) propose guidelines for assigning intellectual property rights and for transferring research results to the private sector; and

''(5) make recommendations for how such entity could be funded from Federal, State, and non-governmental sources.

''(c) COMPOSITION.—In establishing the task force under subsection (a), the Director of the Office of Science and Technology Policy shall appoint an equal number of individuals from institutions of higher education and from industry with knowledge and expertise in cyber-physical systems, and may appoint not more than 2 individuals from Federal laboratories.

''(d) REPORT.—Not later than 1 year after the date of enactment of the Cybersecurity Act of 2012, the Director of the Office of Science and Technology Policy shall transmit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives a report describing the findings and recommendations of the task force.

''(e) TERMINATION.—The task force shall terminate upon transmittal of the report required under subsection (d).

''(f) COMPENSATION AND EXPENSES.—Members of the task force shall serve without compensation.''.

SEC. 303. PROGRAM IMPROVEMENTS.

Section 102 of the High-Performance Computing Act of 1991 (15 U.S.C. 5512) is amended to read as follows:

''SEC. 102. PROGRAM IMPROVEMENTS.

''(a) FUNCTIONS.—The Director of the Office of Science and Technology Policy shall continue—

''(1) to provide technical and administrative support to—

''(A) the agencies participating in planning and implementing the Program, including support needed to develop the strategic plan under section 101(e); and

''(B) the advisory committee under section 101(b);

''(2) to serve as the primary point of contact on Federal networking and information technology activities for government agencies, academia, industry, professional societies, State computing and networking technology programs, interested citizen groups, and others to exchange technical and programmatic information;

''(3) to solicit input and recommendations from a wide range of stakeholders during the development of each strategic plan under section 101(e) by convening at least 1 workshop with invitees from academia, industry, Federal laboratories, and other relevant organizations and institutions;

''(4) to conduct public outreach, including the dissemination of the advisory committee's findings and recommendations, as appropriate;

''(5) to promote access to and early application of the technologies, innovations, and expertise derived from Program activities to

agency missions and systems across the Federal Government and to United States industry;

''(6) to ensure accurate and detailed budget reporting of networking and information technology research and development investment; and

''(7) to encourage agencies participating in the Program to use existing programs and resources to strengthen networking and information technology education and training, and increase participation in such fields, including by women and underrepresented minorities.

''(b) SOURCE OF FUNDING.—

''(1) IN GENERAL.—The functions under this section shall be supported by funds from each agency participating in the Program.

''(2) SPECIFICATIONS.—The portion of the total budget of the Office of Science and Technology Policy that is provided by each agency participating in the Program for each fiscal year shall be in the same proportion as each agency's share of the total budget for the Program for the previous fiscal year, as specified in the database under section 102(c).

''(c) DATABASE.—

''(1) IN GENERAL.—The Director of the Office of Science and Technology Policy shall develop and maintain a database of projects funded by each agency for the fiscal year for each Program Component Area.

''(2) PUBLIC ACCESSIBILITY.—The Director of the Office of Science and Technology Policy shall make the database accessible to the public.

''(3) DATABASE CONTENTS.—The database shall include, for each project in the database—

''(A) a description of the project;

''(B) each agency, industry, institution of higher education, Federal laboratory, or international institution involved in the project;

''(C) the source funding of the project (set forth by agency);

''(D) the funding history of the project; and

''(E) whether the project has been completed.''.

SEC. 304. IMPROVING EDUCATION OF NETWORKING AND INFORMATION TECHNOLOGY, INCLUDING HIGH PERFORMANCE COMPUTING.

Section 201(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)) is amended—

(1) by redesignating paragraphs (2) through (4) as paragraphs (3) through (5), respectively; and

(2) by inserting after paragraph (1) the following:

''(2) the National Science Foundation shall use its existing programs, in collaboration with other agencies, as appropriate, to improve the teaching and learning of networking and information technology at all levels of education and to increase participation in networking and information technology fields;''.

SEC. 305. CONFORMING AND TECHNICAL AMENDMENTS TO THE HIGH-PERFORMANCE COMPUTING ACT OF 1991.

(a) SECTION 3.—Section 3 of the High-Performance Computing Act of 1991 (15 U.S.C. 5502) is amended—

(1) in the matter preceding paragraph (1), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(2) in paragraph (1)—

(A) in the matter preceding subparagraph (A), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(B) in subparagraphs (A), (F), and (G), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(C) in subparagraph (H), by striking ''high-performance'' and inserting ''high-end''; and

(3) in paragraph (2)—

(A) by striking ''high-performance computing and'' and inserting ''networking and information technology, and''; and

(B) by striking ''high-performance computing network'' and inserting ''networking and information technology''.

(b) TITLE HEADING.—The heading of title I of the High-Performance Computing Act of 1991 (105 Stat. 1595) is amended by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''.

(c) SECTION 101.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT**'';

(2) in subsection (a)—

(A) in the subsection heading, by striking ''NATIONAL HIGH-PERFORMANCE COMPUTING'' and inserting ''NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT'';

(B) in paragraph (1)—

(i) by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program'';

(ii) in subparagraph (A), by striking ''high-performance computing, including networking'' and inserting ''networking and information technology'';

(iii) in subparagraphs (B) and (G), by striking ''high-performance'' each place it appears and inserting ''high-end''; and

(iv) in subparagraph (C), by striking ''high-performance computing and networking'' and inserting ''high-end computing, distributed, and networking''; and

(C) in paragraph (2)—

(i) in subparagraphs (A) and (C)—

(I) by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(II) by striking ''development, networking,'' each place it appears and inserting ''development,''; and

(ii) in subparagraphs (G) and (H), as redesignated by section 301(d) of this Act, by striking ''high-performance'' each place it appears and inserting ''high-end'';

(3) in subsection (b)(1), in the matter preceding subparagraph (A), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology research and development'';

(4) in subsection (c)(1)(A), by striking ''high-performance computing'' and inserting ''networking and information technology''.

(d) SECTION 201.—Section 201(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)(1)) is amended by striking ''high-performance computing and advanced high-speed computer networking'' and inserting ''networking and information technology research and development''.

(e) SECTION 202.—Section 202(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5522(a)) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(f) SECTION 203.—Section 203(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5523(a)) is amended—

(1) in paragraph (1), by striking ''high-performance computing and networking'' and inserting ''networking and information technology''; and

(2) in paragraph (2)(A), by striking ''high-performance'' and inserting ''high-end''.

(g) SECTION 204.—Section 204 of the High-Performance Computing Act of 1991 (15 U.S.C. 5524) is amended—

(1) in subsection (a)(1)—

(A) in subparagraph (A), by striking ''high-performance computing systems and networks'' and inserting ''networking and information technology systems and capabilities'';

(B) in subparagraph (B), by striking ''interoperability of high-performance computing systems in networks and for common user interfaces to systems'' and inserting ''interoperability and usability of networking and information technology systems''; and

(C) in subparagraph (C), by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(2) in subsection (b)—

(A) by striking ''HIGH-PERFORMANCE COMPUTING AND NETWORK'' in the heading and inserting ''NETWORKING AND INFORMATION TECHNOLOGY''; and

(B) by striking ''sensitive''.

(h) SECTION 205.—Section 205(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5525(a)) is amended by striking ''computational'' and inserting ''networking and information technology''.

(i) SECTION 206.—Section 206(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5526(a)) is amended by striking ''computational research'' and inserting ''networking and information technology research''.

(j) SECTION 207.—Section 207 of the High-Performance Computing Act of 1991 (15 U.S.C. 5527) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(k) SECTION 208.—Section 208 of the High-Performance Computing Act of 1991 (15 U.S.C. 5528) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''; and

(2) in subsection (a)—

(A) in paragraph (1), by striking ''High-performance computing and associated'' and inserting ''Networking and information'';

(B) in paragraph (2), by striking ''high-performance computing'' and inserting ''networking and information technologies'';

(C) in paragraph (3), by striking ''high-performance'' and inserting ''high-end'';

(D) in paragraph (4), by striking ''high-performance computers and associated'' and inserting ''networking and information''; and

(E) in paragraph (5), by striking ''high-performance computing and associated'' and inserting ''networking and information''.

SEC. 306. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation, in coordination with the Secretary of Homeland Security, shall carry out a Federal cyber scholarship-for-service program to recruit and train the next generation of information technology professionals and security managers to meet the needs of the cybersecurity mission for the Federal government.

(b) PROGRAM DESCRIPTION AND COMPONENTS.—The program shall—

(1) annually assess the workforce needs of the Federal government for cybersecurity professionals, including network engineers, software engineers, and other experts in order to determine how many scholarships should be awarded annually to ensure that the workforce needs following graduation match the number of scholarships awarded;

(2) provide scholarships for up to 1,000 students per year in their pursuit of undergraduate or graduate degrees in the cybersecurity field, in an amount that may include coverage for full tuition, fees, and a stipend;

(3) require each scholarship recipient, as a condition of receiving a scholarship under the program, to serve in a Federal information technology workforce for a period equal

to one and one-half times each year, or partial year, of scholarship received, in addition to an internship in the cybersecurity field, if applicable, following graduation;

(4) provide a procedure for the National Science Foundation or a Federal agency, consistent with regulations of the Office of Personnel Management, to request and fund a security clearance for a scholarship recipient, including providing for clearance during a summer internship and upon graduation; and

(5) provide opportunities for students to receive temporary appointments for meaningful employment in the Federal information technology workforce during school vacation periods and for internships.

(c) HIRING AUTHORITY.—

(1) IN GENERAL.—For purposes of any law or regulation governing the appointment of an individual in the Federal civil service, upon the successful completion of the student's studies, a student receiving a scholarship under the program may—

(A) be hired under section 213.3102(r) of title 5, Code of Federal Regulations; and

(B) be exempt from competitive service.

(2) COMPETITIVE SERVICE.—Upon satisfactory fulfillment of the service term under paragraph (1), an individual may be converted to a competitive service position without competition if the individual meets the requirements for that position.

(d) ELIGIBILITY.—The eligibility requirements for a scholarship under this section shall include that a scholarship applicant—

(1) be a citizen of the United States;

(2) be eligible to be granted a security clearance;

(3) maintain a grade point average of 3.2 or above on a 4.0 scale for undergraduate study or a 3.5 or above on a 4.0 scale for postgraduate study;

(4) demonstrate a commitment to a career in improving the security of the information infrastructure; and

(5) has demonstrated a level of proficiency in math or computer sciences.

(e) FAILURE TO COMPLETE SERVICE OBLIGATION.—

(1) IN GENERAL.—A scholarship recipient under this section shall be liable to the United States under paragraph (2) if the scholarship recipient—

(A) fails to maintain an acceptable level of academic standing in the educational institution in which the individual is enrolled, as determined by the Director;

(B) is dismissed from such educational institution for disciplinary reasons;

(C) withdraws from the program for which the award was made before the completion of such program;

(D) declares that the individual does not intend to fulfill the service obligation under this section;

(E) fails to fulfill the service obligation of the individual under this section; or

(F) loses a security clearance or becomes ineligible for a security clearance.

(2) REPAYMENT AMOUNTS.—

(A) LESS THAN 1 YEAR OF SERVICE.—If a circumstance under paragraph (1) occurs before the completion of 1 year of a service obligation under this section, the total amount of awards received by the individual under this section shall be repaid.

(B) ONE OR MORE YEARS OF SERVICE.—If a circumstance described in subparagraph (D) or (E) of paragraph (1) occurs after the completion of 1 year of a service obligation under this section, the total amount of scholarship awards received by the individual under this section, reduced by the ratio of the number of years of service completed divided by the number of years of service required, shall be repaid.

(f) EVALUATION AND REPORT.—The Director of the National Science Foundation shall—

(1) evaluate the success of recruiting individuals for scholarships under this section and of hiring and retaining those individuals in the public sector workforce, including the annual cost and an assessment of how the program actually improves the Federal workforce; and

(2) periodically report the findings under paragraph (1) to Congress.

(g) AUTHORIZATION OF APPROPRIATIONS.—From amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), the Director may use funds to carry out the requirements of this section for fiscal years 2012 through 2013.

SEC. 307. STUDY AND ANALYSIS OF CERTIFICATION AND TRAINING OF INFORMATION INFRASTRUCTURE PROFESSIONALS.

(a) STUDY.—The President shall enter into an agreement with the National Academies to conduct a comprehensive study of government, academic, and private-sector accreditation, training, and certification programs for personnel working in information infrastructure. The agreement shall require the National Academies to consult with sector coordinating councils and relevant governmental agencies, regulatory entities, and nongovernmental organizations in the course of the study.

(b) SCOPE.—The study shall include—

(1) an evaluation of the body of knowledge and various skills that specific categories of personnel working in information infrastructure should possess in order to secure information systems;

(2) an assessment of whether existing government, academic, and private-sector accreditation, training, and certification programs provide the body of knowledge and various skills described in paragraph (1);

(3) an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity talent, including barriers relating to compensation, the hiring process, job classification, and hiring flexibility; and

(4) an analysis of the sources and availability of cybersecurity talent, a comparison of the skills and expertise sought by the Federal Government and the private sector, an examination of the current and future capacity of United States institutions of higher education, including community colleges, to provide current and future cybersecurity professionals, through education and training activities, with those skills sought by the Federal Government, State and local entities, and the private sector.

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the National Academies shall submit to the President and Congress a report on the results of the study. The report shall include—

(1) findings regarding the state of information infrastructure accreditation, training, and certification programs, including specific areas of deficiency and demonstrable progress; and

(2) recommendations for the improvement of information infrastructure accreditation, training, and certification programs.

SEC. 308. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

(a) IN GENERAL.—The Director of the National Institute of Standards and Technology, in coordination with appropriate Federal authorities, shall—

(1) as appropriate, ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to Congress a plan for ensuring such Federal agency coordination.

(b) CONSULTATION WITH THE PRIVATE SECTOR.—In carrying out the activities under subsection (a)(1), the Director shall ensure consultation with appropriate private sector stakeholders.

SEC. 309. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

The Director of the National Institute of Standards and Technology shall continue a program to support the development of technical standards, metrology, testbeds, and conformance criteria, taking into account appropriate user concerns—

(1) to improve interoperability among identity management technologies;

(2) to strengthen authentication methods of identity management systems;

(3) to improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols; and

(4) to improve the usability of identity management systems.

SEC. 310. FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY RESEARCH GRANT AREAS.—Section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking ''property.'' and inserting ''property;''; and

(3) by adding at the end the following:

''(J) secure fundamental protocols that are at the heart of inter-network communications and data exchange;

''(K) system security that addresses the building of secure systems from trusted and untrusted components;

''(L) monitoring and detection; and

''(M) resiliency and rapid recovery methods.''.

(b) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY GRANTS.—Section 4(a)(3) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(3)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(c) COMPUTER AND NETWORK SECURITY CENTERS.—Section 4(b)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7403(b)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(d) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—Section 5(a)(6) of the Cyber Security Research and Development Act (15 U.S.C. 7404(a)(6)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT GRANTS.—Section 5(b)(2) of the Cyber Security Research and Development Act (15 U.S.C. 7404(b)(2)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(f) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY RESEARCH.—Section 5(c)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7404(c)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

SA 2611. Mrs. HUTCHISON submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 45, strike line 1 and all that follows through page 87, line 22, and insert the following:

TITLE II—COORDINATION OF FEDERAL INFORMATION SECURITY POLICY

SEC. 201. COORDINATION OF FEDERAL INFORMATION SECURITY POLICY.

(a) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by striking subchapters II and III and inserting the following:

''SUBCHAPTER II—INFORMATION SECURITY

''§ 3551. Purposes

''The purposes of this subchapter are—

''(1) to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

''(2) to recognize the highly networked nature of the current Federal computing environment and provide effective government-wide management of policies, directives, standards, and guidelines, as well as effective and nimble oversight of and response to information security risks, including coordination of information security efforts throughout the Federal civilian, national security, and law enforcement communities;

''(3) to provide for development and maintenance of controls required to protect agency information and information systems and contribute to the overall improvement of agency information security posture;

''(4) to provide for the development of tools and methods to assess and respond to real-time situational risk for Federal information system operations and assets; and

''(5) to provide a mechanism for improving agency information security programs through continuous monitoring of agency information systems and streamlined reporting requirements rather than overly prescriptive manual reporting.

''§ 3552. Definitions

''In this subchapter:

''(1) ADEQUATE SECURITY.—The term 'adequate security' means security commensurate with the risk and magnitude of the harm resulting from the unauthorized access to or loss, misuse, destruction, or modification of information.

''(2) AGENCY.—The term 'agency' has the meaning given the term in section 3502 of title 44.

''(3) CYBERSECURITY CENTER.—The term 'cybersecurity center' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

''(4) CYBER THREAT INFORMATION.—The term 'cyber threat information' means information that indicates or describes—

''(A) a technical or operation vulnerability or a cyber threat mitigation measure;

''(B) an action or operation to mitigate a cyber threat;

''(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

''(D) a method of defeating a technical control;

''(E) a method of defeating an operational control;

''(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

''(G) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to inadvertently enable the defeat of a technical or operational control;

''(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

''(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

''(J) any combination of subparagraphs (A) through (I).

''(5) DIRECTOR.—The term 'Director' means the Director of the Office of Management and Budget unless otherwise specified.

''(6) ENVIRONMENT OF OPERATION.—The term 'environment of operation' means the information system and environment in which those systems operate, including changing threats, vulnerabilities, technologies, and missions and business practices.

''(7) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

''(8) INCIDENT.—The term 'incident' means an occurrence that—

''(A) actually or imminently jeopardizes the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores, or transmits; or

''(B) constitutes a violation of law or an imminent threat of violation of a law, a security policy, a security procedure, or an acceptable use policy.

''(9) INFORMATION RESOURCES.—The term 'information resources' has the meaning given the term in section 3502 of title 44.

''(10) INFORMATION SECURITY.—The term 'information security' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

''(A) integrity, by guarding against improper information modification or destruction, including by ensuring information non-repudiation and authenticity;

''(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; or

''(C) availability, by ensuring timely and reliable access to and use of information.

''(11) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44.

''(12) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given the term in section 11101 of title 40.

''(13) MALICIOUS RECONNAISSANCE.—The term 'malicious reconnaissance' means a method for actively probing or passively monitoring an information system for the purpose of discerning technical vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

''(14) NATIONAL SECURITY SYSTEM.—

''(A) IN GENERAL.—The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

''(i) the function, operation, or use of which—

''(I) involves intelligence activities;

''(II) involves cryptologic activities related to national security;

''(III) involves command and control of military forces;

''(IV) involves equipment that is an integral part of a weapon or weapons system; or

''(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

''(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

''(B) LIMITATION.—Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

''(15) OPERATIONAL CONTROL.—The term 'operational control' means a security control for an information system that primarily is implemented and executed by people.

''(16) PERSON.—The term 'person' has the meaning given the term in section 3502 of title 44.

''(17) SECRETARY.—The term 'Secretary' means the Secretary of Commerce unless otherwise specified.

''(18) SECURITY CONTROL.—The term 'security control' means the management, operational, and technical controls, including safeguards or countermeasures, prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

''(19) SIGNIFICANT CYBER INCIDENT.—The term 'significant cyber incident' means a cyber incident resulting in, or an attempted cyber incident that, if successful, would have resulted in—

''(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

''(B) an incident in which an operational or technical control essential to the security or

operation of a Federal information system was defeated.

''(20) TECHNICAL CONTROL.—The term 'technical control' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

''§ 3553. Federal information security authority and coordination

''(a) IN GENERAL.—The Secretary, in consultation with the Secretary of Homeland Security, shall—

''(1) issue compulsory and binding policies and directives governing agency information security operations, and require implementation of such policies and directives, including—

''(A) policies and directives consistent with the standards and guidelines promulgated under section 11331 of title 40 to identify and provide information security protections prioritized and commensurate with the risk and impact resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by or on behalf of an agency; or

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(B) minimum operational requirements for Federal Government to protect agency information systems and provide common situational awareness across all agency information systems;

''(C) reporting requirements, consistent with relevant law, regarding information security incidents and cyber threat information;

''(D) requirements for agencywide information security programs;

''(E) performance requirements and metrics for the security of agency information systems;

''(F) training requirements to ensure that agencies are able to fully and timely comply with the policies and directives issued by the Secretary under this subchapter;

''(G) training requirements regarding privacy, civil rights, and civil liberties, and information oversight for agency information security personnel;

''(H) requirements for the annual reports to the Secretary under section 3554(d);

''(I) any other information security operations or information security requirements as determined by the Secretary in coordination with relevant agency heads; and

''(J) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

''(2) review the agencywide information security programs under section 3554; and

''(3) designate an individual or an entity at each cybersecurity center, among other responsibilities—

''(A) to receive reports and information about information security incidents, cyber threat information, and deterioration of security control affecting agency information systems; and

''(B) to act on or share the information under subparagraph (A) in accordance with this subchapter.

''(b) CONSIDERATIONS.—When issuing policies and directives under subsection (a), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology under section 11331 of title 40.

''(c) LIMITATION OF AUTHORITY.—The authorities of the Secretary under this section shall not apply to national security systems. Information security policies, directives, standards and guidelines for national security systems shall be overseen as directed by the President and, in accordance with that direction, carried out under the authority of the heads of agencies that operate or exercise authority over such national security systems.

''(d) STATUTORY CONSTRUCTION.—Nothing in this subchapter shall be construed to alter or amend any law regarding the authority of any head of an agency over such agency.

''§ 3554. Agency responsibilities

''(a) IN GENERAL.—The head of each agency shall—

''(1) be responsible for—

''(A) complying with the policies and directives issued under section 3553;

''(B) providing information security protections commensurate with the risk resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by the agency or by a contractor of an agency or other organization on behalf of an agency; and

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(C) complying with the requirements of this subchapter, including—

''(i) information security standards and guidelines promulgated under section 11331 of title 40;

''(ii) for any national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued as directed by the President; and

''(iii) for any non-national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued under section 3553;

''(D) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

''(E) reporting and sharing, for an agency operating or exercising control of a national security system, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for national security systems issued as directed by the President; and

''(F) reporting and sharing, for those agencies operating or exercising control of non-national security systems, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for non-national security systems as prescribed under section 3553(a), including information to assist the entity designated under section 3555(a) with the ongoing security analysis under section 3555;

''(2) ensure that each senior agency official provides information security for the information and information systems that support the operations and assets under the senior agency official's control, including by—

''(A) assessing the risk and impact that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

''(B) determining the level of information security appropriate to protect such information and information systems in accordance with policies and directives issued under section 3553(a), and standards and guidelines promulgated under section 11331 of title 40 for information security classifications and related requirements;

''(C) implementing policies, procedures, and capabilities to reduce risks to an acceptable level in a cost-effective manner;

''(D) actively monitoring the effective implementation of information security controls and techniques; and

''(E) reporting information about information security incidents, cyber threat information, and deterioration of security controls in a timely and adequate manner to the entity designated under section 3553(a)(3) in accordance with paragraph (1);

''(3) assess and maintain the resiliency of information technology systems critical to agency mission and operations;

''(4) designate the agency Inspector General (or an independent entity selected in consultation with the Director and the Council of Inspectors General on Integrity and Efficiency if the agency does not have an Inspector General) to conduct the annual independent evaluation required under section 3556, and allow the agency Inspector General to contract with an independent entity to perform such evaluation;

''(5) delegate to the Chief Information Officer or equivalent (or to a senior agency official who reports to the Chief Information Officer or equivalent)—

''(A) the authority and primary responsibility to implement an agencywide information security program; and

''(B) the authority to provide information security for the information collected and maintained by the agency (or by a contractor, other agency, or other source on behalf of the agency) and for the information systems that support the operations, assets, and mission of the agency (including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency);

''(6) delegate to the appropriate agency official (who is responsible for a particular agency system or subsystem) the responsibility to ensure and enforce compliance with all requirements of the agency's agencywide information security program in coordination with the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5);

''(7) ensure that an agency has trained personnel who have obtained any necessary security clearances to permit them to assist the agency in complying with this subchapter;

''(8) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5), in coordination with other senior agency officials, reports to the agency head on the effectiveness of the agencywide information security program, including the progress of any remedial actions; and

''(9) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5) has the necessary qualifications to administer the functions described in this subchapter and has information security duties as a primary duty of that official.

''(b) CHIEF INFORMATION OFFICERS.—Each Chief Information Officer or equivalent (or the senior agency official who reports to the

Chief Information Officer or equivalent) under subsection (a)(5) shall—

''(1) establish and maintain an enterprise security operations capability that on a continuous basis—

''(A) detects, reports, contains, mitigates, and responds to information security incidents that impair adequate security of the agency's information or information system in a timely manner and in accordance with the policies and directives under section 3553; and

''(B) reports any information security incident under subparagraph (A) to the entity designated under section 3555;

''(2) develop, maintain, and oversee an agencywide information security program;

''(3) develop, maintain, and oversee information security policies, procedures, and control techniques to address applicable requirements, including requirements under section 3553 of this title and section 11331 of title 40; and

''(4) train and oversee the agency personnel who have significant responsibility for information security with respect to that responsibility.

''(c) AGENCYWIDE INFORMATION SECURITY PROGRAMS.—

''(1) IN GENERAL.—Each agencywide information security program under subsection (b)(2) shall include—

''(A) relevant security risk assessments, including technical assessments and others related to the acquisition process;

''(B) security testing commensurate with risk and impact;

''(C) mitigation of deterioration of security controls commensurate with risk and impact;

''(D) risk-based continuous monitoring and threat assessment of the operational status and security of agency information systems to enable evaluation of the effectiveness of and compliance with information security policies, procedures, and practices, including a relevant and appropriate selection of security controls of information systems identified in the inventory under section 3505(c);

''(E) operation of appropriate technical capabilities in order to detect, mitigate, report, and respond to information security incidents, cyber threat information, and deterioration of security controls in a manner that is consistent with the policies and directives under section 3553, including—

''(i) mitigating risks associated with such information security incidents;

''(ii) notifying and consulting with the entity designated under section 3555; and

''(iii) notifying and consulting with, as appropriate—

''(I) law enforcement and the relevant Office of the Inspector General; and

''(II) any other entity, in accordance with law and as directed by the President;

''(F) a process to ensure that remedial action is taken to address any deficiencies in the information security policies, procedures, and practices of the agency; and

''(G) a plan and procedures to ensure the continuity of operations for information systems that support the operations and assets of the agency.

''(2) RISK MANAGEMENT STRATEGIES.—Each agencywide information security program under subsection (b)(2) shall include the development and maintenance of a risk management strategy for information security. The risk management strategy shall include—

''(A) consideration of information security incidents, cyber threat information, and deterioration of security controls; and

''(B) consideration of the consequences that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency;

''(3) POLICIES AND PROCEDURES.—Each agencywide information security program under subsection (b)(2) shall include policies and procedures that—

''(A) are based on the risk management strategy under paragraph (2);

''(B) reduce information security risks to an acceptable level in a cost-effective manner;

''(C) ensure that cost-effective and adequate information security is addressed as part of the acquisition and ongoing management of each agency information system; and

''(D) ensure compliance with—

''(i) this subchapter; and

''(ii) any other applicable requirements.

''(4) TRAINING REQUIREMENTS.—Each agencywide information security program under subsection (b)(2) shall include information security, privacy, civil rights, civil liberties, and information oversight training that meets any applicable requirements under section 3553. The training shall inform each information security personnel that has access to agency information systems (including contractors and other users of information systems that support the operations and assets of the agency) of—

''(A) the information security risks associated with the information security personnel's activities; and

''(B) the individual's responsibility to comply with the agency policies and procedures that reduce the risks under subparagraph (A).

''(d) ANNUAL REPORT.—Each agency shall submit a report annually to the Secretary of Homeland Security on its agencywide information security program and information systems.

''§ 3555. Multiagency ongoing threat assessment

''(a) IMPLEMENTATION.—The Director of the Office of Management and Budget, in coordination with the Secretary of Homeland Security, shall designate an entity to implement ongoing security analysis concerning agency information systems—

''(1) based on cyber threat information;

''(2) based on agency information system and environment of operation changes, including—

''(A) an ongoing evaluation of the information system security controls; and

''(B) the security state, risk level, and environment of operation of an agency information system, including—

''(i) a change in risk level due to a new cyber threat;

''(ii) a change resulting from a new technology;

''(iii) a change resulting from the agency's mission; and

''(iv) a change resulting from the business practice; and

''(3) using automated processes to the maximum extent possible—

''(A) to increase information system security;

''(B) to reduce paper-based reporting requirements; and

''(C) to maintain timely and actionable knowledge of the state of the information system security.

''(b) STANDARDS.—The National Institute of Standards and Technology may promulgate standards, in coordination with the Secretary of Homeland Security, to assist an agency with its duties under this section.

''(c) COMPLIANCE.—The head of each appropriate department and agency shall be responsible for ensuring compliance and implementing necessary procedures to comply with this section. The head of each appropriate department and agency, in consultation with the Director of the Office of Management and Budget and the Secretary of Homeland Security, shall—

''(1) monitor compliance under this section;

''(2) develop a timeline and implement for the department or agency—

''(A) adoption of any technology, system, or method that facilitates continuous monitoring and threat assessments of an agency information system;

''(B) adoption or updating of any technology, system, or method that prevents, detects, or remediates a significant cyber incident to a Federal information system of the department or agency that has impeded, or is reasonably likely to impede, the performance of a critical mission of the department or agency; and

''(C) adoption of any technology, system, or method that satisfies a requirement under this section.

''(d) LIMITATION OF AUTHORITY.—The authorities of the Director of the Office of Management and Budget and of the Secretary of Homeland Security under this section shall not apply to national security systems.

''(e) REPORT.—Not later than 6 months after the date of enactment of the Cybersecurity Act of 2012, the Government Accountability Office shall issue a report evaluating each agency's status toward implementing this section.

''§ 3556. Independent evaluations

''(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency, in consultation with the Director and the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense, shall issue and maintain criteria for the timely, cost-effective, risk-based, and independent evaluation of each agencywide information security program (and practices) to determine the effectiveness of the agencywide information security program (and practices). The criteria shall include measures to assess any conflicts of interest in the performance of the evaluation and whether the agencywide information security program includes appropriate safeguards against disclosure of information where such disclosure may adversely affect information security.

''(b) ANNUAL INDEPENDENT EVALUATIONS.—Each agency shall perform an annual independent evaluation of its agencywide information security program (and practices) in accordance with the criteria under subsection (a).

''(c) DISTRIBUTION OF REPORTS.—Not later than 30 days after receiving an independent evaluation under subsection (b), each agency head shall transmit a copy of the independent evaluation to the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense.

''(d) NATIONAL SECURITY SYSTEMS.—Evaluations involving national security systems shall be conducted as directed by President.

''§ 3557. National security systems.

''The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

''(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system; and

''(2) implements information security policies and practices as required by standards and guidelines for national security systems,

issued in accordance with law and as directed by the President.''.

(b) SAVINGS PROVISIONS.—

(1) POLICY AND COMPLIANCE GUIDANCE.—Policy and compliance guidance issued by the Director before the date of enactment of this Act under section 3543(a)(1) of title 44, United States Code (as in effect on the day before the date of enactment of this Act), shall continue in effect, according to its terms, until modified, terminated, superseded, or repealed pursuant to section 3553(a)(1) of title 44, United States Code.

(2) STANDARDS AND GUIDELINES.—Standards and guidelines issued by the Secretary of Commerce or by the Director before the date of enactment of this Act under section 11331(a)(1) of title 40, United States Code, (as in effect on the day before the date of enactment of this Act) shall continue in effect, according to their terms, until modified, terminated, superseded, or repealed pursuant to section 11331(a)(1) of title 40, United States Code, as amended by this Act.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) CHAPTER ANALYSIS.—The chapter analysis for chapter 35 of title 44, United States Code, is amended—

(A) by striking the items relating to sections 3531 through 3538;

(B) by striking the items relating to sections 3541 through 3549; and

(C) by inserting the following:

''3551. Purposes.

''3552. Definitions.

''3553. Federal information security authority and coordination.

''3554. Agency responsibilities.

''3555. Multiagency ongoing threat assessment.

''3556. Independent evaluations.

''3557. National security systems.''.

(2) OTHER REFERENCES.—

(A) Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(1)(A)) is amended by striking ''section 3532(3)'' and inserting ''section 3552''.

(B) Section 2222(j)(5) of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(C) Section 2223(c)(3) of title 10, United States Code, is amended, by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(D) Section 2315 of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(E) Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended—

(i) in subsection (a)(2), by striking ''section 3532(b)(2)'' and inserting ''section 3552'';

(ii) in subsection (c)(3), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iii) in subsection (d)(1), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iv) in subsection (d)(8) by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(v) in subsection (d)(8), by striking ''submitted to the Director'' and inserting ''submitted to the Secretary'';

(vi) in subsection (e)(2), by striking ''section 3532(1) of such title'' and inserting ''section 3552 of title 44''; and

(vii) in subsection (e)(5), by striking ''section 3532(b)(2) of such title'' and inserting ''section 3552 of title 44''.

(F) Section 8(d)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7406(d)(1)) is amended by striking ''section 3534(b)'' and inserting ''section 3554(b)(2)''.

SEC. 202. MANAGEMENT OF INFORMATION TECHNOLOGY.

(a) IN GENERAL.—Section 11331 of title 40, United States Code, is amended to read as follows:

''§ 11331. Responsibilities for Federal information systems standards

''(a) STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO PRESCRIBE.—Except as provided under paragraph (2), the Secretary of Commerce shall prescribe standards and guidelines pertaining to Federal information systems—

''(A) in consultation with the Secretary of Homeland Security; and

''(B) on the basis of standards and guidelines developed by the National Institute of Standards and Technology under paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)(2) and (a)(3)).

''(2) NATIONAL SECURITY SYSTEMS.—Standards and guidelines for national security systems shall be developed, prescribed, enforced, and overseen as otherwise authorized by law and as directed by the President.

''(b) MANDATORY STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO MAKE MANDATORY STANDARDS AND GUIDELINES.—The Secretary of Commerce shall make standards and guidelines under subsection (a)(1) compulsory and binding to the extent determined necessary by the Secretary of Commerce to improve the efficiency of operation or security of Federal information systems.

''(2) REQUIRED MANDATORY STANDARDS AND GUIDELINES.—

''(A) IN GENERAL.—Standards and guidelines under subsection (a)(1) shall include information security standards that—

''(i) provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)); and

''(ii) are otherwise necessary to improve the security of Federal information and information systems.

''(B) BINDING EFFECT.—Information security standards under subparagraph (A) shall be compulsory and binding.

''(c) EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary of Commerce shall exercise the authority conferred by this section subject to direction by the President and in coordination with the Director.

''(d) APPLICATION OF MORE STRINGENT STANDARDS AND GUIDELINES.—The head of an executive agency may employ standards for the cost-effective information security for information systems within or under the supervision of that agency that are more stringent than the standards and guidelines the Secretary of Commerce prescribes under this section if the more stringent standards and guidelines—

''(1) contain at least the applicable standards and guidelines made compulsory and binding by the Secretary of Commerce; and

''(2) are otherwise consistent with the policies, directives, and implementation memoranda issued under section 3553(a) of title 44.

''(e) DECISIONS ON PROMULGATION OF STANDARDS AND GUIDELINES.—The decision by the Secretary of Commerce regarding the promulgation of any standard or guideline under this section shall occur not later than 6 months after the date of submission of the proposed standard to the Secretary of Commerce by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

''(f) NOTICE AND COMMENT.—A decision by the Secretary of Commerce to significantly modify, or not promulgate, a proposed standard submitted to the Secretary by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) shall be made after the public is given an opportunity to comment on the Secretary's proposed decision.

''(g) DEFINITIONS.—In this section:

''(1) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' has the meaning given the term in section 3552 of title 44.

''(2) INFORMATION SECURITY.—The term 'information security' has the meaning given the term in section 3552 of title 44.

''(3) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given the term in section 3552 of title 44.''.

SEC. 203. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 204. TECHNICAL AND CONFORMING AMENDMENTS.

Section 21(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4(b)) is amended—

(1) in paragraph (2), by striking ''and the Director of the Office of Management and Budget'' and inserting '', the Secretary of Commerce, and the Secretary of Homeland Security''; and

(2) in paragraph (3), by inserting '', the Secretary of Homeland Security,'' after ''the Secretary of Commerce''.

SEC. 205. CLARIFICATION OF AUTHORITIES.

Nothing in this title shall be construed to convey any new regulatory authority to any government entity implementing or complying with any provision of this title.

SA 2612. Mrs. HUTCHISON submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 45, strike line 1 and all that follows through the undesignated matter between lines 7 and 8 on page 106, and insert the following:

TITLE II—COORDINATION OF FEDERAL INFORMATION SECURITY POLICY

SEC. 201. COORDINATION OF FEDERAL INFORMATION SECURITY POLICY.

(a) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by striking subchapters II and III and inserting the following:

''SUBCHAPTER II—INFORMATION SECURITY

''§ 3551. Purposes

''The purposes of this subchapter are—

''(1) to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

''(2) to recognize the highly networked nature of the current Federal computing environment and provide effective government-wide management of policies, directives, standards, and guidelines, as well as effective and nimble oversight of and response to information security risks, including coordination of information security efforts throughout the Federal civilian, national security, and law enforcement communities;

''(3) to provide for development and maintenance of controls required to protect agency information and information systems and contribute to the overall improvement of agency information security posture;

''(4) to provide for the development of tools and methods to assess and respond to real-time situational risk for Federal information system operations and assets; and

''(5) to provide a mechanism for improving agency information security programs through continuous monitoring of agency information systems and streamlined reporting requirements rather than overly prescriptive manual reporting.

''§ 3552. Definitions

''In this subchapter:

''(1) ADEQUATE SECURITY.—The term 'adequate security' means security commensurate with the risk and magnitude of the harm resulting from the unauthorized access to or loss, misuse, destruction, or modification of information.

''(2) AGENCY.—The term 'agency' has the meaning given the term in section 3502 of title 44.

''(3) CYBERSECURITY CENTER.—The term 'cybersecurity center' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

''(4) CYBER THREAT INFORMATION.—The term 'cyber threat information' means information that indicates or describes—

''(A) a technical or operation vulnerability or a cyber threat mitigation measure;

''(B) an action or operation to mitigate a cyber threat;

''(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

''(D) a method of defeating a technical control;

''(E) a method of defeating an operational control;

''(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

''(G) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to inadvertently enable the defeat of a technical or operational control;

''(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

''(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

''(J) any combination of subparagraphs (A) through (I).

''(5) DIRECTOR.—The term 'Director' means the Director of the Office of Management and Budget unless otherwise specified.

''(6) ENVIRONMENT OF OPERATION.—The term 'environment of operation' means the information system and environment in which those systems operate, including changing threats, vulnerabilities, technologies, and missions and business practices.

''(7) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

''(8) INCIDENT.—The term 'incident' means an occurrence that—

''(A) actually or imminently jeopardizes the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores, or transmits; or

''(B) constitutes a violation of law or an imminent threat of violation of a law, a security policy, a security procedure, or an acceptable use policy.

''(9) INFORMATION RESOURCES.—The term 'information resources' has the meaning given the term in section 3502 of title 44.

''(10) INFORMATION SECURITY.—The term 'information security' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

''(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

''(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; or

''(C) availability, by ensuring timely and reliable access to and use of information.

''(11) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44.

''(12) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given the term in section 11101 of title 40.

''(13) MALICIOUS RECONNAISSANCE.—The term 'malicious reconnaissance' means a method for actively probing or passively monitoring an information system for the purpose of discerning technical vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

''(14) NATIONAL SECURITY SYSTEM.—

''(A) IN GENERAL.—The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

''(i) the function, operation, or use of which—

''(I) involves intelligence activities;

''(II) involves cryptologic activities related to national security;

''(III) involves command and control of military forces;

''(IV) involves equipment that is an integral part of a weapon or weapons system; or

''(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

''(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

''(B) LIMITATION.—Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

''(15) OPERATIONAL CONTROL.—The term 'operational control' means a security control for an information system that primarily is implemented and executed by people.

''(16) PERSON.—The term 'person' has the meaning given the term in section 3502 of title 44.

''(17) SECRETARY.—The term 'Secretary' means the Secretary of Commerce unless otherwise specified.

''(18) SECURITY CONTROL.—The term 'security control' means the management, operational, and technical controls, including safeguards or countermeasures, prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

''(19) SIGNIFICANT CYBER INCIDENT.—The term 'significant cyber incident' means a cyber incident resulting in, or an attempted cyber incident that, if successful, would have resulted in—

''(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

''(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

''(20) TECHNICAL CONTROL.—The term 'technical control' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

''§ 3553. Federal information security authority and coordination

''(a) IN GENERAL.—The Secretary, in consultation with the Secretary of Homeland Security, shall—

''(1) issue compulsory and binding policies and directives governing agency information security operations, and require implementation of such policies and directives, including—

''(A) policies and directives consistent with the standards and guidelines promulgated under section 11331 of title 40 to identify and provide information security protections prioritized and commensurate with the risk and impact resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by or on behalf of an agency; or

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(B) minimum operational requirements for Federal Government to protect agency information systems and provide common situational awareness across all agency information systems;

''(C) reporting requirements, consistent with relevant law, regarding information security incidents and cyber threat information;

''(D) requirements for agencywide information security programs;

''(E) performance requirements and metrics for the security of agency information systems;

''(F) training requirements to ensure that agencies are able to fully and timely comply with the policies and directives issued by the Secretary under this subchapter;

''(G) training requirements regarding privacy, civil rights, and civil liberties, and information oversight for agency information security personnel;

''(H) requirements for the annual reports to the Secretary under section 3554(d);

''(I) any other information security operations or information security requirements as determined by the Secretary in coordination with relevant agency heads; and

''(J) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

''(2) review the agencywide information security programs under section 3554; and

''(3) designate an individual or an entity at each cybersecurity center, among other responsibilities—

''(A) to receive reports and information about information security incidents, cyber threat information, and deterioration of security control affecting agency information systems; and

''(B) to act on or share the information under subparagraph (A) in accordance with this subchapter.

''(b) CONSIDERATIONS.—When issuing policies and directives under subsection (a), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology under section 11331 of title 40.

''(c) LIMITATION OF AUTHORITY.—The authorities of the Secretary under this section shall not apply to national security systems. Information security policies, directives, standards and guidelines for national security systems shall be overseen as directed by the President and, in accordance with that direction, carried out under the authority of the heads of agencies that operate or exercise authority over such national security systems.

''(d) STATUTORY CONSTRUCTION.—Nothing in this subchapter shall be construed to alter or amend any law regarding the authority of any head of an agency over such agency.

''§ 3554. Agency responsibilities

''(a) IN GENERAL.—The head of each agency shall—

''(1) be responsible for—

''(A) complying with the policies and directives issued under section 3553;

''(B) providing information security protections commensurate with the risk resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by the agency or by a contractor of an agency or other organization on behalf of an agency; and

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(C) complying with the requirements of this subchapter, including—

''(i) information security standards and guidelines promulgated under section 11331 of title 40;

''(ii) for any national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued as directed by the President; and

''(iii) for any non-national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued under section 3553;

''(D) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

''(E) reporting and sharing, for an agency operating or exercising control of a national security system, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for national security systems issued as directed by the President; and

''(F) reporting and sharing, for those agencies operating or exercising control of non-national security systems, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for non-national security systems as prescribed under section 3553(a), including information to assist the entity designated under section 3555(a) with the ongoing security analysis under section 3555;

''(2) ensure that each senior agency official provides information security for the information and information systems that support the operations and assets under the senior agency official's control, including by—

''(A) assessing the risk and impact that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

''(B) determining the level of information security appropriate to protect such information and information systems in accordance with policies and directives issued under section 3553(a), and standards and guidelines promulgated under section 11331 of title 40 for information security classifications and related requirements;

''(C) implementing policies, procedures, and capabilities to reduce risks to an acceptable level in a cost-effective manner;

''(D) actively monitoring the effective implementation of information security controls and techniques; and

''(E) reporting information about information security incidents, cyber threat information, and deterioration of security controls in a timely and adequate manner to the entity designated under section 3553(a)(3) in accordance with paragraph (1);

''(3) assess and maintain the resiliency of information technology systems critical to agency mission and operations;

''(4) designate the agency Inspector General (or an independent entity selected in consultation with the Director and the Council of Inspectors General on Integrity and Efficiency if the agency does not have an Inspector General) to conduct the annual independent evaluation required under section 3556, and allow the agency Inspector General to contract with an independent entity to perform such evaluation;

''(5) delegate to the Chief Information Officer or equivalent (or to a senior agency official who reports to the Chief Information Officer or equivalent)—

''(A) the authority and primary responsibility to implement an agencywide information security program; and

''(B) the authority to provide information security for the information collected and maintained by the agency (or by a contractor, other agency, or other source on behalf of the agency) and for the information systems that support the operations, assets, and mission of the agency (including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency);

''(6) delegate to the appropriate agency official (who is responsible for a particular agency system or subsystem) the responsibility to ensure and enforce compliance with all requirements of the agency's agencywide information security program in coordination with the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5);

''(7) ensure that an agency has trained personnel who have obtained any necessary security clearances to permit them to assist the agency in complying with this subchapter;

''(8) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5), in coordination with other senior agency officials, reports to the agency head on the effectiveness of the agencywide information security program, including the progress of any remedial actions; and

''(9) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5) has the necessary qualifications to administer the functions described in this subchapter and has information security duties as a primary duty of that official.

''(b) CHIEF INFORMATION OFFICERS.—Each Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under subsection (a)(5) shall—

''(1) establish and maintain an enterprise security operations capability that on a continuous basis—

''(A) detects, reports, contains, mitigates, and responds to information security incidents that impair adequate security of the agency's information or information system in a timely manner and in accordance with the policies and directives under section 3553; and

''(B) reports any information security incident under subparagraph (A) to the entity designated under section 3555;

''(2) develop, maintain, and oversee an agencywide information security program;

''(3) develop, maintain, and oversee information security policies, procedures, and control techniques to address applicable requirements, including requirements under section 3553 of this title and section 11331 of title 40; and

''(4) train and oversee the agency personnel who have significant responsibility for information security with respect to that responsibility.

''(c) AGENCYWIDE INFORMATION SECURITY PROGRAMS.—

''(1) IN GENERAL.—Each agencywide information security program under subsection (b)(2) shall include—

''(A) relevant security risk assessments, including technical assessments and others related to the acquisition process;

''(B) security testing commensurate with risk and impact;

''(C) mitigation of deterioration of security controls commensurate with risk and impact;

''(D) risk-based continuous monitoring and threat assessment of the operational status and security of agency information systems to enable evaluation of the effectiveness of and compliance with information security policies, procedures, and practices, including a relevant and appropriate selection of security controls of information systems identified in the inventory under section 3505(c);

''(E) operation of appropriate technical capabilities in order to detect, mitigate, report, and respond to information security incidents, cyber threat information, and deterioration of security controls in a manner that is consistent with the policies and directives under section 3553, including—

''(i) mitigating risks associated with such information security incidents;

''(ii) notifying and consulting with the entity designated under section 3555; and

''(iii) notifying and consulting with, as appropriate—

''(I) law enforcement and the relevant Office of the Inspector General; and

''(II) any other entity, in accordance with law and as directed by the President;

''(F) a process to ensure that remedial action is taken to address any deficiencies in the information security policies, procedures, and practices of the agency; and

''(G) a plan and procedures to ensure the continuity of operations for information systems that support the operations and assets of the agency.

''(2) RISK MANAGEMENT STRATEGIES.—Each agencywide information security program under subsection (b)(2) shall include the development and maintenance of a risk management strategy for information security. The risk management strategy shall include—

''(A) consideration of information security incidents, cyber threat information, and deterioration of security controls; and

''(B) consideration of the consequences that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency;

''(3) POLICIES AND PROCEDURES.—Each agencywide information security program under subsection (b)(2) shall include policies and procedures that—

''(A) are based on the risk management strategy under paragraph (2);

''(B) reduce information security risks to an acceptable level in a cost-effective manner;

''(C) ensure that cost-effective and adequate information security is addressed as part of the acquisition and ongoing management of each agency information system; and

''(D) ensure compliance with—

''(i) this subchapter; and

''(ii) any other applicable requirements.

''(4) TRAINING REQUIREMENTS.—Each agencywide information security program under subsection (b)(2) shall include information security, privacy, civil rights, civil liberties, and information oversight training that meets any applicable requirements under section 3553. The training shall inform each information security personnel that has access to agency information systems (including contractors and other users of information systems that support the operations and assets of the agency) of—

''(A) the information security risks associated with the information security personnel's activities; and

''(B) the individual's responsibility to comply with the agency policies and procedures that reduce the risks under subparagraph (A).

''(d) ANNUAL REPORT.—Each agency shall submit a report annually to the Secretary of Homeland Security on its agencywide information security program and information systems.

''§ 3555. Multiagency ongoing threat assessment

''(a) IMPLEMENTATION.—The Director of the Office of Management and Budget, in coordination with the Secretary of Homeland Security, shall designate an entity to implement ongoing security analysis concerning agency information systems—

''(1) based on cyber threat information;

''(2) based on agency information system and environment of operation changes, including—

''(A) an ongoing evaluation of the information system security controls; and

''(B) the security state, risk level, and environment of operation of an agency information system, including—

''(i) a change in risk level due to a new cyber threat;

''(ii) a change resulting from a new technology;

''(iii) a change resulting from the agency's mission; and

''(iv) a change resulting from the business practice; and

''(3) using automated processes to the maximum extent possible—

''(A) to increase information system security;

''(B) to reduce paper-based reporting requirements; and

''(C) to maintain timely and actionable knowledge of the state of the information system security.

''(b) STANDARDS.—The National Institute of Standards and Technology may promulgate standards, in coordination with the Secretary of Homeland Security, to assist an agency with its duties under this section.

''(c) COMPLIANCE.—The head of each appropriate department and agency shall be responsible for ensuring compliance and implementing necessary procedures to comply with this section. The head of each appropriate department and agency, in consultation with the Director of the Office of Management and Budget and the Secretary of Homeland Security, shall—

''(1) monitor compliance under this section;

''(2) develop a timeline and implement for the department or agency—

''(A) adoption of any technology, system, or method that facilitates continuous monitoring and threat assessments of an agency information system;

''(B) adoption or updating of any technology, system, or method that prevents, detects, or remediates a significant cyber incident to a Federal information system of the department or agency that has impeded, or is reasonably likely to impede, the performance of a critical mission of the department or agency; and

''(C) adoption of any technology, system, or method that satisfies a requirement under this section.

''(d) LIMITATION OF AUTHORITY.—The authorities of the Director of the Office of Management and Budget and of the Secretary of Homeland Security under this section shall not apply to national security systems.

''(e) REPORT.—Not later than 6 months after the date of enactment of the Cybersecurity Act of 2012, the Government Accountability Office shall issue a report evaluating each agency's status toward implementing this section.

''§ 3556. Independent evaluations

''(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency, in consultation with the Director and the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense, shall issue and maintain criteria for the timely, cost-effective, risk-based, and independent evaluation of each agencywide information security program (and practices) to determine the effectiveness of the agencywide information security program (and practices). The criteria shall include measures to assess any conflicts of interest in the performance of the evaluation and whether the agencywide information security program includes appropriate safeguards against disclosure of information where such disclosure may adversely affect information security.

''(b) ANNUAL INDEPENDENT EVALUATIONS.—Each agency shall perform an annual independent evaluation of its agencywide information security program (and practices) in accordance with the criteria under subsection (a).

''(c) DISTRIBUTION OF REPORTS.—Not later than 30 days after receiving an independent evaluation under subsection (b), each agency head shall transmit a copy of the independent evaluation to the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense.

''(d) NATIONAL SECURITY SYSTEMS.—Evaluations involving national security systems shall be conducted as directed by President.

''§ 3557. National security systems.

''The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

''(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system; and

''(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President.''.

(b) SAVINGS PROVISIONS.—

(1) POLICY AND COMPLIANCE GUIDANCE.—Policy and compliance guidance issued by the Director before the date of enactment of this Act under section 3543(a)(1) of title 44, United States Code (as in effect on the day before the date of enactment of this Act), shall continue in effect, according to its terms, until modified, terminated, superseded, or repealed pursuant to section 3553(a)(1) of title 44, United States Code.

(2) STANDARDS AND GUIDELINES.—Standards and guidelines issued by the Secretary of Commerce or by the Director before the date of enactment of this Act under section 11331(a)(1) of title 40, United States Code, (as in effect on the day before the date of enactment of this Act) shall continue in effect, according to their terms, until modified, terminated, superseded, or repealed pursuant to section 11331(a)(1) of title 40, United States Code, as amended by this Act.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) CHAPTER ANALYSIS.—The chapter analysis for chapter 35 of title 44, United States Code, is amended—

(A) by striking the items relating to sections 3531 through 3538;

(B) by striking the items relating to sections 3541 through 3549; and

(C) by inserting the following:

''3551. Purposes.
''3552. Definitions.
''3553. Federal information security authority and coordination.
''3554. Agency responsibilities.
''3555. Multiagency ongoing threat assessment.
''3556. Independent evaluations.
''3557. National security systems.''.

(2) OTHER REFERENCES.—

(A) Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(1)(A)) is amended by striking ''section 3532(3)'' and inserting ''section 3552''.

(B) Section 2222(j)(5) of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(C) Section 2223(c)(3) of title 10, United States Code, is amended, by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(D) Section 2315 of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(E) Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended—

(i) in subsection (a)(2), by striking ''section 3532(b)(2)'' and inserting ''section 3552'';

(ii) in subsection (c)(3), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iii) in subsection (d)(1), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iv) in subsection (d)(8) by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(v) in subsection (d)(8), by striking ''submitted to the Director'' and inserting ''submitted to the Secretary'';

(vi) in subsection (e)(2), by striking ''section 3532(1) of such title'' and inserting ''section 3552 of title 44''; and

(vii) in subsection (e)(5), by striking ''section 3532(b)(2) of such title'' and inserting ''section 3552 of title 44''.

(F) Section 8(d)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7406(d)(1)) is amended by striking ''section 3534(b)'' and inserting ''section 3554(b)(2)''.

SEC. 202. MANAGEMENT OF INFORMATION TECHNOLOGY.

(a) IN GENERAL.—Section 11331 of title 40, United States Code, is amended to read as follows:

''§ 11331. Responsibilities for Federal information systems standards

''(a) STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO PRESCRIBE.—Except as provided under paragraph (2), the Secretary of Commerce shall prescribe standards and guidelines pertaining to Federal information systems—

''(A) in consultation with the Secretary of Homeland Security; and

''(B) on the basis of standards and guidelines developed by the National Institute of Standards and Technology under paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)(2) and (a)(3)).

''(2) NATIONAL SECURITY SYSTEMS.—Standards and guidelines for national security systems shall be developed, prescribed, enforced, and overseen as otherwise authorized by law and as directed by the President.

''(b) MANDATORY STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO MAKE MANDATORY STANDARDS AND GUIDELINES.—The Secretary of Commerce shall make standards and guidelines under subsection (a)(1) compulsory and binding to the extent determined necessary by the Secretary of Commerce to improve the efficiency of operation or security of Federal information systems.

''(2) REQUIRED MANDATORY STANDARDS AND GUIDELINES.—

''(A) IN GENERAL.—Standards and guidelines under subsection (a)(1) shall include information security standards that—

''(i) provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)); and

''(ii) are otherwise necessary to improve the security of Federal information and information systems.

''(B) BINDING EFFECT.—Information security standards under subparagraph (A) shall be compulsory and binding.

''(c) EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary of Commerce shall exercise the authority conferred by this section subject to direction by the President and in coordination with the Director.

''(d) APPLICATION OF MORE STRINGENT STANDARDS AND GUIDELINES.—The head of an executive agency may employ standards for the cost-effective information security for information systems within or under the supervision of that agency that are more stringent than the standards and guidelines the Secretary of Commerce prescribes under this section if the more stringent standards and guidelines—

''(1) contain at least the applicable standards and guidelines made compulsory and binding by the Secretary of Commerce; and

''(2) are otherwise consistent with the policies, directives, and implementation memoranda issued under section 3553(a) of title 44.

''(e) DECISIONS ON PROMULGATION OF STANDARDS AND GUIDELINES.—The decision by the Secretary of Commerce regarding the promulgation of any standard or guideline under this section shall occur not later than 6 months after the date of submission of the proposed standard to the Secretary of Commerce by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

''(f) NOTICE AND COMMENT.—A decision by the Secretary of Commerce to significantly modify, or not promulgate, a proposed standard submitted to the Secretary by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) shall be made after the public is given an opportunity to comment on the Secretary's proposed decision.

''(g) DEFINITIONS.—In this section:

''(1) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' has the meaning given the term in section 3552 of title 44.

''(2) INFORMATION SECURITY.—The term 'information security' has the meaning given the term in section 3552 of title 44.

''(3) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given the term in section 3552 of title 44.''.

SEC. 203. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 204. TECHNICAL AND CONFORMING AMENDMENTS.

Section 21(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4(b)) is amended—

(1) in paragraph (2), by striking ''and the Director of the Office of Management and Budget'' and inserting '', the Secretary of Commerce, and the Secretary of Homeland Security''; and

(2) in paragraph (3), by inserting '', the Secretary of Homeland Security,'' after ''the Secretary of Commerce''.

SEC. 205. CLARIFICATION OF AUTHORITIES.

Nothing in this title shall be construed to convey any new regulatory authority to any government entity implementing or complying with any provision of this title.

SA 2613. Mrs. HUTCHISON (for herself, Mr. MCCAIN, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin) submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 1, strike line 3 and all that follows through page 211, line 6 and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012'' or ''SECURE IT''.

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

TITLE I—FACILITATING SHARING OF CYBER THREAT INFORMATION

SEC. 101. DEFINITIONS.

In this title:

(1) AGENCY.—The term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code.

(2) ANTITRUST LAWS.—The term ''antitrust laws''—

(A) has the meaning given the term in section 1(a) of the Clayton Act (15 U.S.C. 12(a));

(B) includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that section 5 of that Act applies to unfair methods of competition; and

(C) includes any State law that has the same intent and effect as the laws under subparagraphs (A) and (B).

(3) COUNTERMEASURE.—The term ''countermeasure'' means an automated or a manual action with defensive intent to mitigate cyber threats.

(4) CYBER THREAT INFORMATION.—The term ''cyber threat information'' means information that indicates or describes—

(A) a technical or operation vulnerability or a cyber threat mitigation measure;

(B) an action or operation to mitigate a cyber threat;

(C) malicious reconnaissance, including anomalous patterns of network activity that

appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

(D) a method of defeating a technical control;

(E) a method of defeating an operational control;

(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

(G) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to inadvertently enable the defeat of a technical or operational control;

(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

(J) any combination of subparagraphs (A) through (I).

(5) CYBERSECURITY CENTER.—The term ''cybersecurity center'' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

(6) CYBERSECURITY SYSTEM.—The term ''cybersecurity system'' means a system designed or employed to ensure the integrity, confidentiality, or availability of, or to safeguard, a system or network, including measures intended to protect a system or network from—

(A) efforts to degrade, disrupt, or destroy such system or network; or

(B) theft or misappropriations of private or government information, intellectual property, or personally identifiable information.

(7) ENTITY.—

(A) IN GENERAL.—The term ''entity'' means any private entity, non-Federal government agency or department, or State, tribal, or local government agency or department (including an officer, employee, or agent thereof).

(B) INCLUSIONS.—The term ''entity'' includes a government agency or department (including an officer, employee, or agent thereof) of the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States.

(8) FEDERAL INFORMATION SYSTEM.—The term ''Federal information system'' means an information system of a Federal department or agency used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

(9) INFORMATION SECURITY.—The term ''information security'' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; or

(C) availability, by ensuring timely and reliable access to and use of information.

(10) INFORMATION SYSTEM.—The term ''information system'' has the meaning given the term in section 3502 of title 44, United States Code.

(11) LOCAL GOVERNMENT.—The term ''local government'' means any borough, city, county, parish, town, township, village, or other general purpose political subdivision of a State.

(12) MALICIOUS RECONNAISSANCE.—The term ''malicious reconnaissance'' means a method for actively probing or passively monitoring an information system for the purpose of discerning technical vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(13) OPERATIONAL CONTROL.—The term ''operational control'' means a security control for an information system that primarily is implemented and executed by people.

(14) OPERATIONAL VULNERABILITY.—The term ''operational vulnerability'' means any attribute of policy, process, or procedure that could enable or facilitate the defeat of an operational control.

(15) PRIVATE ENTITY.—The term ''private entity'' means any individual or any private group, organization, or corporation, including an officer, employee, or agent thereof.

(16) SIGNIFICANT CYBER INCIDENT.—The term ''significant cyber incident'' means a cyber incident resulting in, or an attempted cyber incident that, if successful, would have resulted in—

(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

(17) TECHNICAL CONTROL.—The term ''technical control'' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

(18) TECHNICAL VULNERABILITY.—The term ''technical vulnerability'' means any attribute of hardware or software that could enable or facilitate the defeat of a technical control.

(19) TRIBAL.—The term ''tribal'' has the meaning given the term ''Indian tribe'' in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

SEC. 102. AUTHORIZATION TO SHARE CYBER THREAT INFORMATION.

(a) VOLUNTARY DISCLOSURE.—

(1) PRIVATE ENTITIES.—Notwithstanding any other provision of law, a private entity may, for the purpose of preventing, investigating, or otherwise mitigating threats to information security, on its own networks, or as authorized by another entity, on such entity's networks, employ countermeasures and use cybersecurity systems in order to obtain, identify, or otherwise possess cyber threat information.

(2) ENTITIES.—Notwithstanding any other provision of law, an entity may disclose cyber threat information to—

(A) a cybersecurity center; or

(B) any other entity in order to assist with preventing, investigating, or otherwise mitigating threats to information security.

(3) INFORMATION SECURITY PROVIDERS.—If the cyber threat information described in paragraph (1) is obtained, identified, or otherwise possessed in the course of providing information security products or services under contract to another entity, that entity shall be given, at any time prior to disclosure of such information, a reasonable opportunity to authorize or prevent such disclosure, to request anonymization of such information, or to request that reasonable efforts be made to safeguard such information that identifies specific persons from unauthorized access or disclosure.

(b) SIGNIFICANT CYBER INCIDENTS INVOLVING FEDERAL INFORMATION SYSTEMS.—

(1) IN GENERAL.—An entity providing electronic communication services, remote computing services, or information security services to a Federal department or agency shall inform the Federal department or agency of a significant cyber incident involving the Federal information system of that Federal department or agency that—

(A) is directly known to the entity as a result of providing such services;

(B) is directly related to the provision of such services by the entity; and

(C) as determined by the entity, has impeded or will impede the performance of a critical mission of the Federal department or agency.

(2) ADVANCE COORDINATION.—A Federal department or agency receiving the services described in paragraph (1) shall coordinate in advance with an entity described in paragraph (1) to develop the parameters of any information that may be provided under paragraph (1), including clarification of the type of significant cyber incident that will impede the performance of a critical mission of the Federal department or agency.

(3) REPORT.—A Federal department or agency shall report information provided under this subsection to a cybersecurity center.

(4) CONSTRUCTION.—Any information provided to a cybersecurity center under paragraph (3) shall be treated in the same manner as information provided to a cybersecurity center under subsection (a).

(c) INFORMATION SHARED WITH OR PROVIDED TO A CYBERSECURITY CENTER.—Cyber threat information provided to a cybersecurity center under this section—

(1) may be disclosed to, retained by, and used by, consistent with otherwise applicable Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal government for a cybersecurity purpose, a national security purpose, or in order to prevent, investigate, or prosecute any of the offenses listed in section 2516 of title 18, United States Code, and such information shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under this paragraph;

(2) may, with the prior written consent of the entity submitting such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(3) shall be considered the commercial, financial, or proprietary information of the entity providing such information to the Federal government and any disclosure outside the Federal government may only be made upon the prior written consent by such entity and shall not constitute a waiver of any applicable privilege or protection provided by law, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(4) shall be deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records;

(5) shall be, without discretion, withheld from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records;

(6) shall not be subject to the rules of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official;

(7) shall not, if subsequently provided to a State, tribal, or local government or government agency, otherwise be disclosed or distributed to any entity by such State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent; and

(8) shall not be directly used by any Federal, State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph.

(d) PROCEDURES RELATING TO INFORMATION SHARING WITH A CYBERSECURITY CENTER.—Not later than 60 days after the date of enactment of this Act, the heads of each department or agency containing a cybersecurity center shall jointly develop, promulgate, and submit to Congress procedures to ensure that cyber threat information shared with or provided to—

(1) a cybersecurity center under this section—

(A) may be submitted to a cybersecurity center by an entity, to the greatest extent possible, through a uniform, publicly available process or format that is easily accessible on the website of such cybersecurity center, and that includes the ability to provide relevant details about the cyber threat information and written consent to any subsequent disclosures authorized by this paragraph;

(B) shall immediately be further shared with each cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government;

(C) is handled by the Federal government in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title, and the Federal government may undertake efforts consistent with this subparagraph to limit the impact on privacy and civil liberties of the sharing of cyber threat information with the Federal government; and

(D) except as provided in this section, shall only be used, disclosed, or handled in accordance with the provisions of subsection (c); and

(2) a Federal agency or department under subsection (b) is provided immediately to a cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government.

(e) INFORMATION SHARED BETWEEN ENTITIES.—

(1) IN GENERAL.—An entity sharing cyber threat information with another entity under this title may restrict the use or sharing of such information by such other entity.

(2) FURTHER SHARING.—Cyber threat information shared by any entity with another entity under this title—

(A) shall only be further shared in accordance with any restrictions placed on the sharing of such information by the entity authorizing such sharing, such as appropriate anonymization of such information; and

(B) may not be used by any entity to gain an unfair competitive advantage to the detriment of the entity authorizing the sharing of such information, except that the conduct described in paragraph (3) shall not constitute unfair competitive conduct.

(3) INFORMATION SHARED WITH STATE, TRIBAL, OR LOCAL GOVERNMENT OR GOVERNMENT AGENCY.—Cyber threat information shared with a State, tribal, or local government or government agency under this title—

(A) may, with the prior written consent of the entity sharing such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent;

(B) shall be deemed voluntarily shared information and exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records;

(C) shall not be disclosed or distributed to any entity by the State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent; and

(D) shall not be directly used by any State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this subparagraph.

(4) ANTITRUST EXEMPTION.—The exchange or provision of cyber threat information or assistance between 2 or more private entities under this title shall not be considered a violation of any provision of antitrust laws if exchanged or provided in order to assist with—

(A) facilitating the prevention, investigation, or mitigation of threats to information security; or

(B) communicating or disclosing of cyber threat information to help prevent, investigate or otherwise mitigate the effects of a threat to information security.

(5) NO RIGHT OR BENEFIT.—The provision of cyber threat information to an entity under this section shall not create a right or a benefit to similar information by such entity or any other entity.

(f) FEDERAL PREEMPTION.—

(1) IN GENERAL.—This section supersedes any statute or other law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this section.

(2) STATE LAW ENFORCEMENT.—Nothing in this section shall be construed to supersede any statute or other law of a State or political subdivision of a State concerning the use of authorized law enforcement techniques.

(3) PUBLIC DISCLOSURE.—No information shared with or provided to a State, tribal, or local government or government agency pursuant to this section shall be made publicly available pursuant to any State, tribal, or local law requiring disclosure of information or records.

(g) CIVIL AND CRIMINAL LIABILITY.—

(1) GENERAL PROTECTIONS.—

(A) PRIVATE ENTITIES.—No cause of action shall lie or be maintained in any court against any private entity for—

(i) the use of countermeasures and cybersecurity systems as authorized by this title;

(ii) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(iii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such private entity.

(B) ENTITIES.—No cause of action shall lie or be maintained in any court against any entity for—

(i) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(ii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such entity.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed as creating any immunity against, or otherwise affecting, any action brought by the Federal government, or any agency or department thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, and use of classified information.

(h) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this section shall be construed to limit or prohibit otherwise lawful disclosures of communications, records, or other information by a private entity to any other governmental or private entity not covered under this section.

(i) WHISTLEBLOWER PROTECTION.—Nothing in this Act shall be construed to preempt or preclude any employee from exercising rights currently provided under any whistleblower law, rule, or regulation.

(j) RELATIONSHIP TO OTHER LAWS.—The submission of cyber threat information under this section to a cybersecurity center shall not affect any requirement under any other provision of law for an entity to provide information to the Federal government.

SEC. 103. INFORMATION SHARING BY THE FEDERAL GOVERNMENT.

(a) CLASSIFIED INFORMATION.—

(1) PROCEDURES.—Consistent with the protection of intelligence sources and methods, and as otherwise determined appropriate, the Director of National Intelligence and the Secretary of Defense, in consultation with the heads of the appropriate Federal departments or agencies, shall develop and promulgate procedures to facilitate and promote—

(A) the immediate sharing, through the cybersecurity centers, of classified cyber threat information in the possession of the Federal government with appropriately cleared representatives of any appropriate entity; and

(B) the declassification and immediate sharing, through the cybersecurity centers, with any entity or, if appropriate, public availability of cyber threat information in the possession of the Federal government;

(2) HANDLING OF CLASSIFIED INFORMATION.—The procedures developed under paragraph (1) shall ensure that each entity receiving classified cyber threat information pursuant to this section has acknowledged in writing the ongoing obligation to comply with all

laws, executive orders, and procedures concerning the appropriate handling, disclosure, or use of classified information.

(b) UNCLASSIFIED CYBER THREAT INFORMATION.—The heads of each department or agency containing a cybersecurity center shall jointly develop and promulgate procedures that ensure that, consistent with the provisions of this section, unclassified, including controlled unclassified, cyber threat information in the possession of the Federal government—

(1) is shared, through the cybersecurity centers, in an immediate and adequate manner with appropriate entities; and

(2) if appropriate, is made publicly available.

(c) DEVELOPMENT OF PROCEDURES.—

(1) IN GENERAL.—The procedures developed under this section shall incorporate, to the greatest extent possible, existing processes utilized by sector specific information sharing and analysis centers.

(2) COORDINATION WITH ENTITIES.—In developing the procedures required under this section, the Director of National Intelligence and the heads of each department or agency containing a cybersecurity center shall coordinate with appropriate entities to ensure that protocols are implemented that will facilitate and promote the sharing of cyber threat information by the Federal government.

(d) ADDITIONAL RESPONSIBILITIES OF CYBERSECURITY CENTERS.—Consistent with section 102, a cybersecurity center shall—

(1) facilitate information sharing, interaction, and collaboration among and between cybersecurity centers and—

(A) other Federal entities;

(B) any entity; and

(C) international partners, in consultation with the Secretary of State;

(2) disseminate timely and actionable cybersecurity threat, vulnerability, mitigation, and warning information, including alerts, advisories, indicators, signatures, and mitigation and response measures, to improve the security and protection of information systems; and

(3) coordinate with other Federal entities, as appropriate, to integrate information from across the Federal government to provide situational awareness of the cybersecurity posture of the United States.

(e) SHARING WITHIN THE FEDERAL GOVERNMENT.—The heads of appropriate Federal departments and agencies shall ensure that cyber threat information in the possession of such Federal departments or agencies that relates to the prevention, investigation, or mitigation of threats to information security across the Federal government is shared effectively with the cybersecurity centers.

(f) SUBMISSION TO CONGRESS.—Not later than 60 days after the date of enactment of this Act, the Director of National Intelligence, in coordination with the appropriate head of a department or an agency containing a cybersecurity center, shall submit the procedures required by this section to Congress.

SEC. 104. CONSTRUCTION.

(a) INFORMATION SHARING RELATIONSHIPS.—Nothing in this title shall be construed—

(1) to limit or modify an existing information sharing relationship;

(2) to prohibit a new information sharing relationship;

(3) to require a new information sharing relationship between any entity and the Federal government, except as specified under section 102(b); or

(4) to modify the authority of a department or agency of the Federal government to protect sources and methods and the national security of the United States.

(b) ANTI-TASKING RESTRICTION.—Nothing in this title shall be construed to permit the Federal government—

(1) to require an entity to share information with the Federal government, except as expressly provided under section 102(b); or

(2) to condition the sharing of cyber threat information with an entity on such entity's provision of cyber threat information to the Federal government.

(c) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this title shall be construed to subject any entity to liability for choosing not to engage in the voluntary activities authorized under this title.

(d) USE AND RETENTION OF INFORMATION.—Nothing in this title shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal government to retain or use any information shared under section 102 for any use other than a use permitted under subsection 102(c)(1).

(e) NO NEW FUNDING.—An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 105. REPORT ON IMPLEMENTATION.

(a) CONTENT OF REPORT.—Not later than 1 year after the date of enactment of this Act, and biennially thereafter, the heads of each department or agency containing a cybersecurity center shall jointly submit, in coordination with the privacy and civil liberties officials of such departments or agencies and the Privacy and Civil Liberties Oversight Board, a detailed report to Congress concerning the implementation of this title, including—

(1) an assessment of the sufficiency of the procedures developed under section 103 of this Act in ensuring that cyber threat information in the possession of the Federal government is provided in an immediate and adequate manner to appropriate entities or, if appropriate, is made publicly available;

(2) an assessment of whether information has been appropriately classified and an accounting of the number of security clearances authorized by the Federal government for purposes of this title;

(3) a review of the type of cyber threat information shared with a cybersecurity center under section 102 of this Act, including whether such information meets the definition of cyber threat information under section 101, the degree to which such information may impact the privacy and civil liberties of individuals, any appropriate metrics to determine any impact of the sharing of such information with the Federal government on privacy and civil liberties, and the adequacy of any steps taken to reduce such impact;

(4) a review of actions taken by the Federal government based on information provided to a cybersecurity center under section 102 of this Act, including the appropriateness of any subsequent use under section 102(c)(1) of this Act and whether there was inappropriate stovepiping within the Federal government of any such information;

(5) a description of any violations of the requirements of this title by the Federal government;

(6) a classified list of entities that received classified information from the Federal government under section 103 of this Act and a description of any indication that such information may not have been appropriately handled;

(7) a summary of any breach of information security, if known, attributable to a specific failure by any entity or the Federal government to act on cyber threat information in the possession of such entity or the Federal government that resulted in substantial economic harm or injury to a specific entity or the Federal government; and

(8) any recommendation for improvements or modifications to the authorities under this title.

(b) FORM OF REPORT.—The report under subsection (a) shall be submitted in unclassified form, but shall include a classified annex.

SEC. 106. INSPECTOR GENERAL REVIEW.

(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency are authorized to review compliance by the cybersecurity centers, and by any Federal department or agency receiving cyber threat information from such cybersecurity centers, with the procedures required under section 102 of this Act.

(b) SCOPE OF REVIEW.—The review under subsection (a) shall consider whether the Federal government has handled such cyber threat information in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title.

(c) REPORT TO CONGRESS.—Each review conducted under this section shall be provided to Congress not later than 30 days after the date of completion of the review.

SEC. 107. TECHNICAL AMENDMENTS.

Section 552(b) of title 5, United States Code, is amended—

(1) in paragraph (8), by striking ''or'';

(2) in paragraph (9), by striking ''wells.'' and inserting ''wells; or''; and

(3) by adding at the end the following:

''(10) information shared with or provided to a cybersecurity center under section 102 of title I of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012.''.

SEC. 108. ACCESS TO CLASSIFIED INFORMATION.

(a) AUTHORIZATION REQUIRED.—No person shall be provided with access to classified information (as defined in section 6.1 of Executive Order 13526 (50 U.S.C. 435 note; relating to classified national security information)) relating to cyber security threats or cyber security vulnerabilities under this title without the appropriate security clearances.

(b) SECURITY CLEARANCES.—The appropriate Federal agencies or departments shall, consistent with applicable procedures and requirements, and if otherwise deemed appropriate, assist an individual in timely obtaining an appropriate security clearance where such individual has been determined to be eligible for such clearance and has a need-to-know (as defined in section 6.1 of that Executive Order) classified information to carry out this title.

TITLE II—COORDINATION OF FEDERAL INFORMATION SECURITY POLICY

SEC. 201. COORDINATION OF FEDERAL INFORMATION SECURITY POLICY.

(a) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by striking subchapters II and III and inserting the following:

''SUBCHAPTER II—INFORMATION SECURITY

''§ 3551. Purposes

''The purposes of this subchapter are—

''(1) to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

''(2) to recognize the highly networked nature of the current Federal computing environment and provide effective government-wide management of policies, directives, standards, and guidelines, as well as effective and nimble oversight of and response to

information security risks, including coordination of information security efforts throughout the Federal civilian, national security, and law enforcement communities;

''(3) to provide for development and maintenance of controls required to protect agency information and information systems and contribute to the overall improvement of agency information security posture;

''(4) to provide for the development of tools and methods to assess and respond to real-time situational risk for Federal information system operations and assets; and

''(5) to provide a mechanism for improving agency information security programs through continuous monitoring of agency information systems and streamlined reporting requirements rather than overly prescriptive manual reporting.

''§ 3552. Definitions

''In this subchapter:

''(1) ADEQUATE SECURITY.—The term 'adequate security' means security commensurate with the risk and magnitude of the harm resulting from the unauthorized access to or loss, misuse, destruction, or modification of information.

''(2) AGENCY.—The term 'agency' has the meaning given the term in section 3502 of title 44.

''(3) CYBERSECURITY CENTER.—The term 'cybersecurity center' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

''(4) CYBER THREAT INFORMATION.—The term 'cyber threat information' means information that indicates or describes—

''(A) a technical or operation vulnerability or a cyber threat mitigation measure;

''(B) an action or operation to mitigate a cyber threat;

''(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

''(D) a method of defeating a technical control;

''(E) a method of defeating an operational control;

''(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

''(G) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to inadvertently enable the defeat of a technical or operational control;

''(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

''(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

''(J) any combination of subparagraphs (A) through (I).

''(5) DIRECTOR.—The term 'Director' means the Director of the Office of Management and Budget unless otherwise specified.

''(6) ENVIRONMENT OF OPERATION.—The term 'environment of operation' means the information system and environment in which those systems operate, including changing threats, vulnerabilities, technologies, and missions and business practices.

''(7) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

''(8) INCIDENT.—The term 'incident' means an occurrence that—

''(A) actually or imminently jeopardizes the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores, or transmits; or

''(B) constitutes a violation of law or an imminent threat of violation of a law, a security policy, a security procedure, or an acceptable use policy.

''(9) INFORMATION RESOURCES.—The term 'information resources' has the meaning given the term in section 3502 of title 44.

''(10) INFORMATION SECURITY.—The term 'information security' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

''(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

''(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; or

''(C) availability, by ensuring timely and reliable access to and use of information.

''(11) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44.

''(12) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given the term in section 11101 of title 40.

''(13) MALICIOUS RECONNAISSANCE.—The term 'malicious reconnaissance' means a method for actively probing or passively monitoring an information system for the purpose of discerning technical vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

''(14) NATIONAL SECURITY SYSTEM.—

''(A) IN GENERAL.—The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

''(i) the function, operation, or use of which—

''(I) involves intelligence activities;

''(II) involves cryptologic activities related to national security;

''(III) involves command and control of military forces;

''(IV) involves equipment that is an integral part of a weapon or weapons system; or

''(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

''(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

''(B) LIMITATION.—Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

''(15) OPERATIONAL CONTROL.—The term 'operational control' means a security control for an information system that primarily is implemented and executed by people.

''(16) PERSON.—The term 'person' has the meaning given the term in section 3502 of title 44.

''(17) SECRETARY.—The term 'Secretary' means the Secretary of Commerce unless otherwise specified.

''(18) SECURITY CONTROL.—The term 'security control' means the management, operational, and technical controls, including safeguards or countermeasures, prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

''(19) SIGNIFICANT CYBER INCIDENT.—The term 'significant cyber incident' means a cyber incident resulting in, or an attempted cyber incident that, if successful, would have resulted in—

''(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

''(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

''(20) TECHNICAL CONTROL.—The term 'technical control' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

''§ 3553. Federal information security authority and coordination

''(a) IN GENERAL.—The Secretary, in consultation with the Secretary of Homeland Security, shall—

''(1) issue compulsory and binding policies and directives governing agency information security operations, and require implementation of such policies and directives, including—

''(A) policies and directives consistent with the standards and guidelines promulgated under section 11331 of title 40 to identify and provide information security protections prioritized and commensurate with the risk and impact resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by or on behalf of an agency; or

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(B) minimum operational requirements for Federal Government to protect agency information systems and provide common situational awareness across all agency information systems;

''(C) reporting requirements, consistent with relevant law, regarding information security incidents and cyber threat information;

''(D) requirements for agencywide information security programs;

''(E) performance requirements and metrics for the security of agency information systems;

''(F) training requirements to ensure that agencies are able to fully and timely comply with the policies and directives issued by the Secretary under this subchapter;

''(G) training requirements regarding privacy, civil rights, and civil liberties, and information oversight for agency information security personnel;

''(H) requirements for the annual reports to the Secretary under section 3554(d);

''(I) any other information security operations or information security requirements as determined by the Secretary in coordination with relevant agency heads; and

''(J) coordinating the development of standards and guidelines under section 20 of

the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

''(2) review the agencywide information security programs under section 3554; and

''(3) designate an individual or an entity at each cybersecurity center, among other responsibilities—

''(A) to receive reports and information about information security incidents, cyber threat information, and deterioration of security control affecting agency information systems; and

''(B) to act on or share the information under subparagraph (A) in accordance with this subchapter.

''(b) CONSIDERATIONS.—When issuing policies and directives under subsection (a), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology under section 11331 of title 40.

''(c) LIMITATION OF AUTHORITY.—The authorities of the Secretary under this section shall not apply to national security systems. Information security policies, directives, standards and guidelines for national security systems shall be overseen as directed by the President and, in accordance with that direction, carried out under the authority of the heads of agencies that operate or exercise authority over such national security systems.

''(d) STATUTORY CONSTRUCTION.—Nothing in this subchapter shall be construed to alter or amend any law regarding the authority of any head of an agency over such agency.

''§ 3554. Agency responsibilities

''(a) IN GENERAL.—The head of each agency shall—

''(1) be responsible for—

''(A) complying with the policies and directives issued under section 3553;

''(B) providing information security protections commensurate with the risk resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by the agency or by a contractor of an agency or other organization on behalf of an agency; and

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(C) complying with the requirements of this subchapter, including—

''(i) information security standards and guidelines promulgated under section 11331 of title 40;

''(ii) for any national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued as directed by the President; and

''(iii) for any non-national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued under section 3553;

''(D) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

''(E) reporting and sharing, for an agency operating or exercising control of a national security system, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for national security systems issued as directed by the President; and

''(F) reporting and sharing, for those agencies operating or exercising control of non-national security systems, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for non-national security systems as prescribed under section 3553(a), including information to assist the entity designated under section 3555(a) with the ongoing security analysis under section 3555;

''(2) ensure that each senior agency official provides information security for the information and information systems that support the operations and assets under the senior agency official's control, including by—

''(A) assessing the risk and impact that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

''(B) determining the level of information security appropriate to protect such information and information systems in accordance with policies and directives issued under section 3553(a), and standards and guidelines promulgated under section 11331 of title 40 for information security classifications and related requirements;

''(C) implementing policies, procedures, and capabilities to reduce risks to an acceptable level in a cost-effective manner;

''(D) actively monitoring the effective implementation of information security controls and techniques; and

''(E) reporting information about information security incidents, cyber threat information, and deterioration of security controls in a timely and adequate manner to the entity designated under section 3553(a)(3) in accordance with paragraph (1);

''(3) assess and maintain the resiliency of information technology systems critical to agency mission and operations;

''(4) designate the agency Inspector General (or an independent entity selected in consultation with the Director and the Council of Inspectors General on Integrity and Efficiency if the agency does not have an Inspector General) to conduct the annual independent evaluation required under section 3556, and allow the agency Inspector General to contract with an independent entity to perform such evaluation;

''(5) delegate to the Chief Information Officer or equivalent (or to a senior agency official who reports to the Chief Information Officer or equivalent)—

''(A) the authority and primary responsibility to implement an agencywide information security program; and

''(B) the authority to provide information security for the information collected and maintained by the agency (or by a contractor, other agency, or other source on behalf of the agency) and for the information systems that support the operations, assets, and mission of the agency (including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency);

''(6) delegate to the appropriate agency official (who is responsible for a particular agency system or subsystem) the responsibility to ensure and enforce compliance with all requirements of the agency's agencywide information security program in coordination with the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5);

''(7) ensure that an agency has trained personnel who have obtained any necessary security clearances to permit them to assist the agency in complying with this subchapter;

''(8) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5), in coordination with other senior agency officials, reports to the agency head on the effectiveness of the agencywide information security program, including the progress of any remedial actions; and

''(9) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5) has the necessary qualifications to administer the functions described in this subchapter and has information security duties as a primary duty of that official.

''(b) CHIEF INFORMATION OFFICERS.—Each Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under subsection (a)(5) shall—

''(1) establish and maintain an enterprise security operations capability that on a continuous basis—

''(A) detects, reports, contains, mitigates, and responds to information security incidents that impair adequate security of the agency's information or information system in a timely manner and in accordance with the policies and directives under section 3553; and

''(B) reports any information security incident under subparagraph (A) to the entity designated under section 3555;

''(2) develop, maintain, and oversee an agencywide information security program;

''(3) develop, maintain, and oversee information security policies, procedures, and control techniques to address applicable requirements, including requirements under section 3553 of this title and section 11331 of title 40; and

''(4) train and oversee the agency personnel who have significant responsibility for information security with respect to that responsibility.

''(c) AGENCYWIDE INFORMATION SECURITY PROGRAMS.—

''(1) IN GENERAL.—Each agencywide information security program under subsection (b)(2) shall include—

''(A) relevant security risk assessments, including technical assessments and others related to the acquisition process;

''(B) security testing commensurate with risk and impact;

''(C) mitigation of deterioration of security controls commensurate with risk and impact;

''(D) risk-based continuous monitoring and threat assessment of the operational status and security of agency information systems to enable evaluation of the effectiveness of and compliance with information security policies, procedures, and practices, including a relevant and appropriate selection of security controls of information systems identified in the inventory under section 3505(c);

''(E) operation of appropriate technical capabilities in order to detect, mitigate, report, and respond to information security incidents, cyber threat information, and deterioration of security controls in a manner that is consistent with the policies and directives under section 3553, including—

''(i) mitigating risks associated with such information security incidents;

''(ii) notifying and consulting with the entity designated under section 3555; and

''(iii) notifying and consulting with, as appropriate—

''(I) law enforcement and the relevant Office of the Inspector General; and

''(II) any other entity, in accordance with law and as directed by the President;

''(F) a process to ensure that remedial action is taken to address any deficiencies in the information security policies, procedures, and practices of the agency; and

''(G) a plan and procedures to ensure the continuity of operations for information systems that support the operations and assets of the agency.

''(2) RISK MANAGEMENT STRATEGIES.—Each agencywide information security program under subsection (b)(2) shall include the development and maintenance of a risk management strategy for information security. The risk management strategy shall include—

''(A) consideration of information security incidents, cyber threat information, and deterioration of security controls; and

''(B) consideration of the consequences that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency;

''(3) POLICIES AND PROCEDURES.—Each agencywide information security program under subsection (b)(2) shall include policies and procedures that—

''(A) are based on the risk management strategy under paragraph (2);

''(B) reduce information security risks to an acceptable level in a cost-effective manner;

''(C) ensure that cost-effective and adequate information security is addressed as part of the acquisition and ongoing management of each agency information system; and

''(D) ensure compliance with—

''(i) this subchapter; and

''(ii) any other applicable requirements.

''(4) TRAINING REQUIREMENTS.—Each agencywide information security program under subsection (b)(2) shall include information security, privacy, civil rights, civil liberties, and information oversight training that meets any applicable requirements under section 3553. The training shall inform each information security personnel that has access to agency information systems (including contractors and other users of information systems that support the operations and assets of the agency) of—

''(A) the information security risks associated with the information security personnel's activities; and

''(B) the individual's responsibility to comply with the agency policies and procedures that reduce the risks under subparagraph (A).

''(d) ANNUAL REPORT.—Each agency shall submit a report annually to the Secretary of Homeland Security on its agencywide information security program and information systems.

''§ 3555. Multiagency ongoing threat assessment

''(a) IMPLEMENTATION.—The Director of the Office of Management and Budget, in coordination with the Secretary of Homeland Security, shall designate an entity to implement ongoing security analysis concerning agency information systems—

''(1) based on cyber threat information;

''(2) based on agency information system and environment of operation changes, including—

''(A) an ongoing evaluation of the information system security controls; and

''(B) the security state, risk level, and environment of operation of an agency information system, including—

''(i) a change in risk level due to a new cyber threat;

''(ii) a change resulting from a new technology;

''(iii) a change resulting from the agency's mission; and

''(iv) a change resulting from the business practice; and

''(3) using automated processes to the maximum extent possible—

''(A) to increase information system security;

''(B) to reduce paper-based reporting requirements; and

''(C) to maintain timely and actionable knowledge of the state of the information system security.

''(b) STANDARDS.—The National Institute of Standards and Technology may promulgate standards, in coordination with the Secretary of Homeland Security, to assist an agency with its duties under this section.

''(c) COMPLIANCE.—The head of each appropriate department and agency shall be responsible for ensuring compliance and implementing necessary procedures to comply with this section. The head of each appropriate department and agency, in consultation with the Director of the Office of Management and Budget and the Secretary of Homeland Security, shall—

''(1) monitor compliance under this section;

''(2) develop a timeline and implement for the department or agency—

''(A) adoption of any technology, system, or method that facilitates continuous monitoring and threat assessments of an agency information system;

''(B) adoption or updating of any technology, system, or method that prevents, detects, or remediates a significant cyber incident to a Federal information system of the department or agency that has impeded, or is reasonably likely to impede, the performance of a critical mission of the department or agency; and

''(C) adoption of any technology, system, or method that satisfies a requirement under this section.

''(d) LIMITATION OF AUTHORITY.—The authorities of the Director of the Office of Management and Budget and of the Secretary of Homeland Security under this section shall not apply to national security systems.

''(e) REPORT.—Not later than 6 months after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Government Accountability Office shall issue a report evaluating each agency's status toward implementing this section.

''§ 3556. Independent evaluations

''(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency, in consultation with the Director and the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense, shall issue and maintain criteria for the timely, cost-effective, risk-based, and independent evaluation of each agencywide information security program (and practices) to determine the effectiveness of the agencywide information security program (and practices). The criteria shall include measures to assess any conflicts of interest in the performance of the evaluation and whether the agencywide information security program includes appropriate safeguards against disclosure of information where such disclosure may adversely affect information security.

''(b) ANNUAL INDEPENDENT EVALUATIONS.—Each agency shall perform an annual independent evaluation of its agencywide information security program (and practices) in accordance with the criteria under subsection (a).

''(c) DISTRIBUTION OF REPORTS.—Not later than 30 days after receiving an independent evaluation under subsection (b), each agency head shall transmit a copy of the independent evaluation to the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense.

''(d) NATIONAL SECURITY SYSTEMS.—Evaluations involving national security systems shall be conducted as directed by President.

''§ 3557. National security systems.

''The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

''(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system; and

''(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President.''.

(b) SAVINGS PROVISIONS.—

(1) POLICY AND COMPLIANCE GUIDANCE.—Policy and compliance guidance issued by the Director before the date of enactment of this Act under section 3543(a)(1) of title 44, United States Code (as in effect on the day before the date of enactment of this Act), shall continue in effect, according to its terms, until modified, terminated, superseded, or repealed pursuant to section 3553(a)(1) of title 44, United States Code.

(2) STANDARDS AND GUIDELINES.—Standards and guidelines issued by the Secretary of Commerce or by the Director before the date of enactment of this Act under section 11331(a)(1) of title 40, United States Code, (as in effect on the day before the date of enactment of this Act) shall continue in effect, according to their terms, until modified, terminated, superseded, or repealed pursuant to section 11331(a)(1) of title 40, United States Code, as amended by this Act.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) CHAPTER ANALYSIS.—The chapter analysis for chapter 35 of title 44, United States Code, is amended—

(A) by striking the items relating to sections 3531 through 3538;

(B) by striking the items relating to sections 3541 through 3549; and

(C) by inserting the following:

''3551. Purposes.
''3552. Definitions.
''3553. Federal information security authority and coordination.
''3554. Agency responsibilities.
''3555. Multiagency ongoing threat assessment.
''3556. Independent evaluations.
''3557. National security systems.''.

(2) OTHER REFERENCES.—

(A) Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(1)(A)) is amended by striking ''section 3532(3)'' and inserting ''section 3552''.

(B) Section 2222(j)(5) of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(C) Section 2223(c)(3) of title 10, United States Code, is amended, by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(D) Section 2315 of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(E) Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended—

(i) in subsection (a)(2), by striking ''section 3532(b)(2)'' and inserting ''section 3552'';

(ii) in subsection (c)(3), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iii) in subsection (d)(1), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iv) in subsection (d)(8) by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(v) in subsection (d)(8), by striking ''submitted to the Director'' and inserting ''submitted to the Secretary'';

(vi) in subsection (e)(2), by striking ''section 3532(1) of such title'' and inserting ''section 3552 of title 44''; and

(vii) in subsection (e)(5), by striking ''section 3532(b)(2) of such title'' and inserting ''section 3552 of title 44''.

(F) Section 8(d)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7406(d)(1)) is amended by striking ''section 3534(b)'' and inserting ''section 3554(b)(2)''.

SEC. 202. MANAGEMENT OF INFORMATION TECHNOLOGY.

(a) IN GENERAL.—Section 11331 of title 40, United States Code, is amended to read as follows:

''§ 11331. Responsibilities for Federal information systems standards

''(a) STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO PRESCRIBE.—Except as provided under paragraph (2), the Secretary of Commerce shall prescribe standards and guidelines pertaining to Federal information systems—

''(A) in consultation with the Secretary of Homeland Security; and

''(B) on the basis of standards and guidelines developed by the National Institute of Standards and Technology under paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)(2) and (a)(3)).

''(2) NATIONAL SECURITY SYSTEMS.—Standards and guidelines for national security systems shall be developed, prescribed, enforced, and overseen as otherwise authorized by law and as directed by the President.

''(b) MANDATORY STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO MAKE MANDATORY STANDARDS AND GUIDELINES.—The Secretary of Commerce shall make standards and guidelines under subsection (a)(1) compulsory and binding to the extent determined necessary by the Secretary of Commerce to improve the efficiency of operation or security of Federal information systems.

''(2) REQUIRED MANDATORY STANDARDS AND GUIDELINES.—

''(A) IN GENERAL.—Standards and guidelines under subsection (a)(1) shall include information security standards that—

''(i) provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)); and

''(ii) are otherwise necessary to improve the security of Federal information and information systems.

''(B) BINDING EFFECT.—Information security standards under subparagraph (A) shall be compulsory and binding.

''(c) EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary of Commerce shall exercise the authority conferred by this section subject to direction by the President and in coordination with the Director.

''(d) APPLICATION OF MORE STRINGENT STANDARDS AND GUIDELINES.—The head of an executive agency may employ standards for the cost-effective information security for information systems within or under the supervision of that agency that are more stringent than the standards and guidelines the Secretary of Commerce prescribes under this section if the more stringent standards and guidelines—

''(1) contain at least the applicable standards and guidelines made compulsory and binding by the Secretary of Commerce; and

''(2) are otherwise consistent with the policies, directives, and implementation memoranda issued under section 3553(a) of title 44.

''(e) DECISIONS ON PROMULGATION OF STANDARDS AND GUIDELINES.—The decision by the Secretary of Commerce regarding the promulgation of any standard or guideline under this section shall occur not later than 6 months after the date of submission of the proposed standard to the Secretary of Commerce by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

''(f) NOTICE AND COMMENT.—A decision by the Secretary of Commerce to significantly modify, or not promulgate, a proposed standard submitted to the Secretary by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) shall be made after the public is given an opportunity to comment on the Secretary's proposed decision.

''(g) DEFINITIONS.—In this section:

''(1) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' has the meaning given the term in section 3552 of title 44.

''(2) INFORMATION SECURITY.—The term 'information security' has the meaning given the term in section 3552 of title 44.

''(3) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given the term in section 3552 of title 44.''.

SEC. 203. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 204. TECHNICAL AND CONFORMING AMENDMENTS.

Section 21(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4(b)) is amended—

(1) in paragraph (2), by striking ''and the Director of the Office of Management and Budget'' and inserting '', the Secretary of Commerce, and the Secretary of Homeland Security''; and

(2) in paragraph (3), by inserting '', the Secretary of Homeland Security,'' after ''the Secretary of Commerce''.

SEC. 205. CLARIFICATION OF AUTHORITIES.

Nothing in this title shall be construed to convey any new regulatory authority to any government entity implementing or complying with any provision of this title.

TITLE III—CRIMINAL PENALTIES

SEC. 301. PENALTIES FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030(c) of title 18, United States Code, is amended to read as follows:

''(c) The punishment for an offense under subsection (a) or (b) of this section is—

''(1) a fine under this title or imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(1) of this section;

''(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than 3 years, or both, in the case of an offense under subsection (a)(2); or

''(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2) of this section, if—

''(i) the offense was committed for purposes of commercial advantage or private financial gain;

''(ii) the offense was committed in the furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States, or of any State; or

''(iii) the value of the information obtained, or that would have been obtained if the offense was completed, exceeds $5,000;

''(3) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(3) of this section;

''(4) a fine under this title or imprisonment of not more than 20 years, or both, in the case of an offense under subsection (a)(4) of this section;

''(5)(A) except as provided in subparagraph (C), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A) of this section, if the offense caused—

''(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

''(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

''(iii) physical injury to any person;

''(iv) a threat to public health or safety;

''(v) damage affecting a computer used by, or on behalf of, an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

''(vi) damage affecting 10 or more protected computers during any 1-year period;

''(B) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(B), if the offense caused a harm provided in clause (i) through (vi) of subparagraph (A) of this subsection;

''(C) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both;

''(D) a fine under this title, imprisonment for not more than 10 years, or both, for any other offense under subsection (a)(5);

''(E) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(6) of this section; or

''(F) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(7) of this section.''.

SEC. 302. TRAFFICKING IN PASSWORDS.

Section 1030(a)(6) of title 18, United States Code, is amended to read as follows:

''(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information or means of access through which a protected computer (as defined in subparagraphs (A) and (B) of subsection (e)(2)) may be accessed without authorization.''.

SEC. 303. CONSPIRACY AND ATTEMPTED COMPUTER FRAUD OFFENSES.

Section 1030(b) of title 18, United States Code, is amended by inserting ''as if for the completed offense'' after ''punished as provided''.

SEC. 304. CRIMINAL AND CIVIL FORFEITURE FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030 of title 18, United States Code, is amended by striking subsections (i) and (j) and inserting the following:

''(i) CRIMINAL FORFEITURE.—

''(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

''(A) such persons interest in any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of such violation; and

''(B) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of such violation.

''(2) The criminal forfeiture of property under this subsection, including any seizure and disposition of the property, and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

''(j) CIVIL FORFEITURE.—

''(1) The following shall be subject to forfeiture to the United States and no property right, real or personal, shall exist in them:

''(A) Any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of any violation of this section, or a conspiracy to violate this section.

''(B) Any property, real or personal, constituting or derived from any gross proceeds obtained directly or indirectly, or any property traceable to such property, as a result of the commission of any violation of this section, or a conspiracy to violate this section.

''(2) Seizures and forfeitures under this subsection shall be governed by the provisions in chapter 46 relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents and other persons as may be designated for that purpose by the Secretary of Homeland Security or the Attorney General.''.

SEC. 305. DAMAGE TO CRITICAL INFRASTRUCTURE COMPUTERS.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

''§ 1030A. Aggravated damage to a critical infrastructure computer

''(a) DEFINITIONS.—In this section—

''(1) the term 'computer' has the meaning given the term in section 1030;

''(2) the term 'critical infrastructure computer' means a computer that manages or controls systems or assets vital to national defense, national security, national economic security, public health or safety, or any combination of those matters, whether publicly or privately owned or operated, including—

''(A) oil and gas production, storage, conversion, and delivery systems;

''(B) water supply systems;

''(C) telecommunication networks;

''(D) electrical power generation and delivery systems;

''(E) finance and banking systems;

''(F) emergency services;

''(G) transportation systems and services; and

''(H) government operations that provide essential services to the public; and

''(3) the term 'damage' has the meaning given the term in section 1030.

''(b) OFFENSE.—It shall be unlawful, during and in relation to a felony violation of section 1030, to knowingly cause or attempt to cause damage to a critical infrastructure computer if the damage results in (or, in the case of an attempt, if completed, would have resulted in) the substantial impairment—

''(1) of the operation of the critical infrastructure computer; or

''(2) of the critical infrastructure associated with the computer.

''(c) PENALTY.—Any person who violates subsection (b) shall be—

''(1) fined under this title;

''(2) imprisoned for not less than 3 years but not more than 20 years; or

''(3) penalized under paragraphs (1) and (2).

''(d) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

''(1) a court shall not place on probation any person convicted of a violation of this section;

''(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment, including any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for a felony violation of section 1030;

''(3) in determining any term of imprisonment to be imposed for a felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The chapter analysis for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

''1030A. Aggravated damage to a critical infrastructure computer.''.

SEC. 306. LIMITATION ON ACTIONS INVOLVING UNAUTHORIZED USE.

Section 1030(e)(6) of title 18, United States Code, is amended by striking ''alter;'' and inserting ''alter, but does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized;''.

SEC. 307. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

TITLE IV—CYBERSECURITY RESEARCH AND DEVELOPMENT

SEC. 401. NATIONAL HIGH-PERFORMANCE COMPUTING PROGRAM PLANNING AND COORDINATION.

(a) GOALS AND PRIORITIES.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(d) GOALS AND PRIORITIES.—The goals and priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include—

''(1) encouraging and supporting mechanisms for interdisciplinary research and development in networking and information technology, including—

''(A) through collaborations across agencies;

''(B) through collaborations across Program Component Areas;

''(C) through collaborations with industry;

''(D) through collaborations with institutions of higher education;

''(E) through collaborations with Federal laboratories (as defined in section 4 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3703)); and

''(F) through collaborations with international organizations;

''(2) addressing national, multi-agency, multi-faceted challenges of national importance; and

''(3) fostering the transfer of research and development results into new technologies and applications for the benefit of society.''.

(b) DEVELOPMENT OF STRATEGIC PLAN.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(e) STRATEGIC PLAN.—

''(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the agencies under subsection (a)(3)(B), working through the National Science and Technology Council and with the assistance of the Office of Science and Technology Policy shall develop a 5-year strategic plan to guide the activities under subsection (a)(1).

''(2) CONTENTS.—The strategic plan shall specify—

''(A) the near-term objectives for the Program;

''(B) the long-term objectives for the Program;

''(C) the anticipated time frame for achieving the near-term objectives;

''(D) the metrics that will be used to assess any progress made toward achieving the near-term objectives and the long-term objectives; and

''(E) how the Program will achieve the goals and priorities under subsection (d).

''(3) IMPLEMENTATION ROADMAP.—

''(A) IN GENERAL.—The agencies under subsection (a)(3)(B) shall develop and annually update an implementation roadmap for the strategic plan.

''(B) REQUIREMENTS.—The information in the implementation roadmap shall be coordinated with the database under section 102(c) and the annual report under section 101(a)(3). The implementation roadmap shall—

''(i) specify the role of each Federal agency in carrying out or sponsoring research and development to meet the research objectives of the strategic plan, including a description of how progress toward the research objectives will be evaluated, with consideration of any relevant recommendations of the advisory committee;

''(ii) specify the funding allocated to each major research objective of the strategic plan and the source of funding by agency for the current fiscal year; and

''(iii) estimate the funding required for each major research objective of the strategic plan for the next 3 fiscal years.

''(4) RECOMMENDATIONS.—The agencies under subsection (a)(3)(B) shall take into consideration when developing the strategic plan under paragraph (1) the recommendations of—

''(A) the advisory committee under subsection (b); and

''(B) the stakeholders under section 102(a)(3).

''(5) REPORT TO CONGRESS.—The Director of the Office of Science and Technology Policy shall transmit the strategic plan under this

subsection, including the implementation roadmap and any updates under paragraph (3), to—

''(A) the advisory committee under subsection (b);

''(B) the Committee on Commerce, Science, and Transportation of the Senate; and

''(C) the Committee on Science and Technology of the House of Representatives.''.

(c) PERIODIC REVIEWS.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(f) PERIODIC REVIEWS.—The agencies under subsection (a)(3)(B) shall—

''(1) periodically assess the contents and funding levels of the Program Component Areas and restructure the Program when warranted, taking into consideration any relevant recommendations of the advisory committee under subsection (b); and

''(2) ensure that the Program includes national, multi-agency, multi-faceted research and development activities, including activities described in section 104.''.

(d) ADDITIONAL RESPONSIBILITIES OF DIRECTOR.—Section 101(a)(2) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(2)) is amended—

(1) by redesignating subparagraphs (E) and (F) as subparagraphs (G) and (H), respectively; and

(2) by inserting after subparagraph (D) the following:

''(E) encourage and monitor the efforts of the agencies participating in the Program to allocate the level of resources and management attention necessary—

''(i) to ensure that the strategic plan under subsection (e) is developed and executed effectively; and

''(ii) to ensure that the objectives of the Program are met;

''(F) working with the Office of Management and Budget and in coordination with the creation of the database under section 102(c), direct the Office of Science and Technology Policy and the agencies participating in the Program to establish a mechanism (consistent with existing law) to track all ongoing and completed research and development projects and associated funding;''.

(e) ADVISORY COMMITTEE.—Section 101(b) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(b)) is amended—

(1) in paragraph (1)—

(A) by inserting after the first sentence the following: ''The co-chairs of the advisory committee shall meet the qualifications of committee members and may be members of the Presidents Council of Advisors on Science and Technology.''; and

(B) by striking ''high-performance'' in subparagraph (D) and inserting ''high-end''; and

(2) by amending paragraph (2) to read as follows:

''(2) In addition to the duties under paragraph (1), the advisory committee shall conduct periodic evaluations of the funding, management, coordination, implementation, and activities of the Program. The advisory committee shall report its findings and recommendations not less frequently than once every 3 fiscal years to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives. The report shall be submitted in conjunction with the update of the strategic plan.''.

(f) REPORT.—Section 101(a)(3) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(3)) is amended—

(1) in subparagraph (C)—

(A) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(B) by striking ''each Program Component Area'' and inserting ''each Program Component Area and each research area supported in accordance with section 104'';

(2) in subparagraph (D)—

(A) by striking ''each Program Component Area,'' and inserting ''each Program Component Area and each research area supported in accordance with section 104,'';

(B) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(C) by striking ''and'' after the semicolon;

(3) by redesignating subparagraph (E) as subparagraph (G); and

(4) by inserting after subparagraph (D) the following:

''(E) include a description of how the objectives for each Program Component Area, and the objectives for activities that involve multiple Program Component Areas, relate to the objectives of the Program identified in the strategic plan under subsection (e);

''(F) include—

''(i) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the next fiscal year by category of activity;

''(ii) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the current fiscal year by category of activity; and

''(iii) the amount of funding provided for the Office of Science and Technology Policy for the current fiscal year by each agency participating in the Program; and''.

(g) DEFINITIONS.—Section 4 of the High-Performance Computing Act of 1991 (15 U.S.C. 5503) is amended—

(1) by redesignating paragraphs (1) and (2) as paragraphs (2) and (3), respectively;

(2) by redesignating paragraph (3) as paragraph (6);

(3) by redesignating paragraphs (6) and (7) as paragraphs (7) and (8), respectively;

(4) by inserting before paragraph (2), as redesignated, the following:

''(1) 'cyber-physical systems' means physical or engineered systems whose networking and information technology functions and physical elements are deeply integrated and are actively connected to the physical world through sensors, actuators, or other means to perform monitoring and control functions;'';

(5) in paragraph (3), as redesignated, by striking ''high-performance computing'' and inserting ''networking and information technology'';

(6) in paragraph (6), as redesignated—

(A) by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(B) by striking ''supercomputer'' and inserting ''high-end computing'';

(7) in paragraph (5), by striking ''network referred to as'' and all that follows through the semicolon and inserting ''network, including advanced computer networks of Federal agencies and departments''; and

(8) in paragraph (7), as redesignated, by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program''.

SEC. 402. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

(a) RESEARCH IN AREAS OF NATIONAL IMPORTANCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.) is amended by adding at the end the following:

''SEC. 104. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

''(a) IN GENERAL.—The Program shall encourage agencies under section 101(a)(3)(B) to support, maintain, and improve national, multi-agency, multi-faceted, research and development activities in networking and information technology directed toward application areas that have the potential for significant contributions to national economic competitiveness and for other significant societal benefits.

''(b) TECHNICAL SOLUTIONS.—An activity under subsection (a) shall be designed to advance the development of research discoveries by demonstrating technical solutions to important problems in areas including—

''(1) cybersecurity;

''(2) health care;

''(3) energy management and low-power systems and devices;

''(4) transportation, including surface and air transportation;

''(5) cyber-physical systems;

''(6) large-scale data analysis and modeling of physical phenomena;

''(7) large scale data analysis and modeling of behavioral phenomena;

''(8) supply chain quality and security; and

''(9) privacy protection and protected disclosure of confidential data.

''(c) RECOMMENDATIONS.—The advisory committee under section 101(b) shall make recommendations to the Program for candidate research and development areas for support under this section.

''(d) CHARACTERISTICS.—

''(1) IN GENERAL.—Research and development activities under this section—

''(A) shall include projects selected on the basis of applications for support through a competitive, merit-based process;

''(B) shall leverage, when possible, Federal investments through collaboration with related State initiatives;

''(C) shall include a plan for fostering the transfer of research discoveries and the results of technology demonstration activities, including from institutions of higher education and Federal laboratories, to industry for commercial development;

''(D) shall involve collaborations among researchers in institutions of higher education and industry; and

''(E) may involve collaborations among nonprofit research institutions and Federal laboratories, as appropriate.

''(2) COST-SHARING.—In selecting applications for support, the agencies under section 101(a)(3)(B) shall give special consideration to projects that include cost sharing from non-Federal sources.

''(3) MULTIDISCIPLINARY RESEARCH CENTERS.—Research and development activities under this section shall be supported through multidisciplinary research centers, including Federal laboratories, that are organized to investigate basic research questions and carry out technology demonstration activities in areas described in subsection (a). Research may be carried out through existing multidisciplinary centers, including those authorized under section 7024(b)(2) of the America COMPETES Act (42 U.S.C. 1862o–10(2)).''.

(b) CYBER-PHYSICAL SYSTEMS.—Section 101(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following:

''(J) provide for increased understanding of the scientific principles of cyber-physical systems and improve the methods available for the design, development, and operation of cyber-physical systems that are characterized by high reliability, safety, and security; and

''(K) provide for research and development on human-computer interactions, visualization, and big data.''.

(c) TASK FORCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.), as amended by section 402(a) of this Act, is amended by adding at the end the following:

''SEC. 105. TASK FORCE.

''(a) ESTABLISHMENT.—Not later than 180 days after the date of enactment the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy under section 102 shall convene a task force to explore mechanisms for carrying out collaborative research and development activities for cyber-physical systems (including the related technologies required to enable these systems) through a consortium or other appropriate entity with participants from institutions of higher education, Federal laboratories, and industry.

''(b) FUNCTIONS.—The task force shall—

''(1) develop options for a collaborative model and an organizational structure for such entity under which the joint research and development activities could be planned, managed, and conducted effectively, including mechanisms for the allocation of resources among the participants in such entity for support of such activities;

''(2) propose a process for developing a research and development agenda for such entity, including guidelines to ensure an appropriate scope of work focused on nationally significant challenges and requiring collaboration and to ensure the development of related scientific and technological milestones;

''(3) define the roles and responsibilities for the participants from institutions of higher education, Federal laboratories, and industry in such entity;

''(4) propose guidelines for assigning intellectual property rights and for transferring research results to the private sector; and

''(5) make recommendations for how such entity could be funded from Federal, State, and non-governmental sources.

''(c) COMPOSITION.—In establishing the task force under subsection (a), the Director of the Office of Science and Technology Policy shall appoint an equal number of individuals from institutions of higher education and from industry with knowledge and expertise in cyber-physical systems, and may appoint not more than 2 individuals from Federal laboratories.

''(d) REPORT.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy shall transmit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives a report describing the findings and recommendations of the task force.

''(e) TERMINATION.—The task force shall terminate upon transmittal of the report required under subsection (d).

''(f) COMPENSATION AND EXPENSES.—Members of the task force shall serve without compensation.''.

SEC. 403. PROGRAM IMPROVEMENTS.

Section 102 of the High-Performance Computing Act of 1991 (15 U.S.C. 5512) is amended to read as follows:

''SEC. 102. PROGRAM IMPROVEMENTS.

''(a) FUNCTIONS.—The Director of the Office of Science and Technology Policy shall continue—

''(1) to provide technical and administrative support to—

''(A) the agencies participating in planning and implementing the Program, including support needed to develop the strategic plan under section 101(e); and

''(B) the advisory committee under section 101(b);

''(2) to serve as the primary point of contact on Federal networking and information technology activities for government agencies, academia, industry, professional societies, State computing and networking technology programs, interested citizen groups, and others to exchange technical and programmatic information;

''(3) to solicit input and recommendations from a wide range of stakeholders during the development of each strategic plan under section 101(e) by convening at least 1 workshop with invitees from academia, industry, Federal laboratories, and other relevant organizations and institutions;

''(4) to conduct public outreach, including the dissemination of the advisory committee's findings and recommendations, as appropriate;

''(5) to promote access to and early application of the technologies, innovations, and expertise derived from Program activities to agency missions and systems across the Federal Government and to United States industry;

''(6) to ensure accurate and detailed budget reporting of networking and information technology research and development investment; and

''(7) to encourage agencies participating in the Program to use existing programs and resources to strengthen networking and information technology education and training, and increase participation in such fields, including by women and underrepresented minorities.

''(b) SOURCE OF FUNDING.—

''(1) IN GENERAL.—The functions under this section shall be supported by funds from each agency participating in the Program.

''(2) SPECIFICATIONS.—The portion of the total budget of the Office of Science and Technology Policy that is provided by each agency participating in the Program for each fiscal year shall be in the same proportion as each agency's share of the total budget for the Program for the previous fiscal year, as specified in the database under section 102(c).

''(c) DATABASE.—

''(1) IN GENERAL.—The Director of the Office of Science and Technology Policy shall develop and maintain a database of projects funded by each agency for the fiscal year for each Program Component Area.

''(2) PUBLIC ACCESSIBILITY.—The Director of the Office of Science and Technology Policy shall make the database accessible to the public.

''(3) DATABASE CONTENTS.—The database shall include, for each project in the database—

''(A) a description of the project;

''(B) each agency, industry, institution of higher education, Federal laboratory, or international institution involved in the project;

''(C) the source funding of the project (set forth by agency);

''(D) the funding history of the project; and

''(E) whether the project has been completed.''.

SEC. 404. IMPROVING EDUCATION OF NETWORKING AND INFORMATION TECHNOLOGY, INCLUDING HIGH PERFORMANCE COMPUTING.

Section 201(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)) is amended—

(1) by redesignating paragraphs (2) through (4) as paragraphs (3) through (5), respectively; and

(2) by inserting after paragraph (1) the following:

''(2) the National Science Foundation shall use its existing programs, in collaboration with other agencies, as appropriate, to improve the teaching and learning of networking and information technology at all levels of education and to increase participation in networking and information technology fields;''.

SEC. 405. CONFORMING AND TECHNICAL AMENDMENTS TO THE HIGH-PERFORMANCE COMPUTING ACT OF 1991.

(a) SECTION 3.—Section 3 of the High-Performance Computing Act of 1991 (15 U.S.C. 5502) is amended—

(1) in the matter preceding paragraph (1), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(2) in paragraph (1)—

(A) in the matter preceding subparagraph (A), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(B) in subparagraphs (A), (F), and (G), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(C) in subparagraph (H), by striking ''high-performance'' and inserting ''high-end''; and

(3) in paragraph (2)—

(A) by striking ''high-performance computing and'' and inserting ''networking and information technology, and''; and

(B) by striking ''high-performance computing network'' and inserting ''networking and information technology''.

(b) TITLE HEADING.—The heading of title I of the High-Performance Computing Act of 1991 (105 Stat. 1595) is amended by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''.

(c) SECTION 101.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT**'';

(2) in subsection (a)—

(A) in the subsection heading, by striking ''NATIONAL HIGH-PERFORMANCE COMPUTING'' and inserting ''NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT'';

(B) in paragraph (1)—

(i) by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program'';

(ii) in subparagraph (A), by striking ''high-performance computing, including networking'' and inserting ''networking and information technology'';

(iii) in subparagraphs (B) and (G), by striking ''high-performance'' each place it appears and inserting ''high-end''; and

(iv) in subparagraph (C), by striking ''high-performance computing and networking'' and inserting ''high-end computing, distributed, and networking''; and

(C) in paragraph (2)—

(i) in subparagraphs (A) and (C)—

(I) by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(II) by striking ''development, networking,'' each place it appears and inserting ''development,''; and

(ii) in subparagraphs (G) and (H), as redesignated by section 401(d) of this Act, by striking ''high-performance'' each place it appears and inserting ''high-end'';

(3) in subsection (b)(1), in the matter preceding subparagraph (A), by striking ''high-

performance computing'' each place it appears and inserting ''networking and information technology''; and

(4) in subsection (c)(1)(A), by striking ''high-performance computing'' and inserting ''networking and information technology''.

(d) SECTION 201.—Section 201(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)(1)) is amended by striking ''high-performance computing and advanced high-speed computer networking'' and inserting ''networking and information technology research and development''.

(e) SECTION 202.—Section 202(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5522(a)) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(f) SECTION 203.—Section 203(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5523(a)) is amended—

(1) in paragraph (1), by striking ''high-performance computing and networking'' and inserting ''networking and information technology''; and

(2) in paragraph (2)(A), by striking ''high-performance'' and inserting ''high-end''.

(g) SECTION 204.—Section 204 of the High-Performance Computing Act of 1991 (15 U.S.C. 5524) is amended—

(1) in subsection (a)(1)—

(A) in subparagraph (A), by striking ''high-performance computing systems and networks'' and inserting ''networking and information technology systems and capabilities'';

(B) in subparagraph (B), by striking ''interoperability of high-performance computing systems in networks and for common user interfaces to systems'' and inserting ''interoperability and usability of networking and information technology systems''; and

(C) in subparagraph (C), by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(2) in subsection (b)—

(A) by striking ''HIGH-PERFORMANCE COMPUTING AND NETWORK'' in the heading and inserting ''NETWORKING AND INFORMATION TECHNOLOGY''; and

(B) by striking ''sensitive''.

(h) SECTION 205.—Section 205(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5525(a)) is amended by striking ''computational'' and inserting ''networking and information technology''.

(i) SECTION 206.—Section 206(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5526(a)) is amended by striking ''computational research'' and inserting ''networking and information technology research''.

(j) SECTION 207.—Section 207 of the High-Performance Computing Act of 1991 (15 U.S.C. 5527) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(k) SECTION 208.—Section 208 of the High-Performance Computing Act of 1991 (15 U.S.C. 5528) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''; and

(2) in subsection (a)—

(A) in paragraph (1), by striking ''High-performance computing and associated'' and inserting ''Networking and information'';

(B) in paragraph (2), by striking ''high-performance computing'' and inserting ''networking and information technologies'';

(C) in paragraph (3), by striking ''high-performance'' and inserting ''high-end'';

(D) in paragraph (4), by striking ''high-performance computers and associated'' and inserting ''networking and information''; and

(E) in paragraph (5), by striking ''high-performance computing and associated'' and inserting ''networking and information''.

SEC. 406. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation, in coordination with the Secretary of Homeland Security, shall carry out a Federal cyber scholarship-for-service program to recruit and train the next generation of information technology professionals and security managers to meet the needs of the cybersecurity mission for the Federal government.

(b) PROGRAM DESCRIPTION AND COMPONENTS.—The program shall—

(1) annually assess the workforce needs of the Federal government for cybersecurity professionals, including network engineers, software engineers, and other experts in order to determine how many scholarships should be awarded annually to ensure that the workforce needs following graduation match the number of scholarships awarded;

(2) provide scholarships for up to 1,000 students per year in their pursuit of undergraduate or graduate degrees in the cybersecurity field, in an amount that may include coverage for full tuition, fees, and a stipend;

(3) require each scholarship recipient, as a condition of receiving a scholarship under the program, to serve in a Federal information technology workforce for a period equal to one and one-half times each year, or partial year, of scholarship received, in addition to an internship in the cybersecurity field, if applicable, following graduation;

(4) provide a procedure for the National Science Foundation or a Federal agency, consistent with regulations of the Office of Personnel Management, to request and fund a security clearance for a scholarship recipient, including providing for clearance during a summer internship and upon graduation; and

(5) provide opportunities for students to receive temporary appointments for meaningful employment in the Federal information technology workforce during school vacation periods and for internships.

(c) HIRING AUTHORITY.—

(1) IN GENERAL.—For purposes of any law or regulation governing the appointment of an individual in the Federal civil service, upon the successful completion of the student's studies, a student receiving a scholarship under the program may—

(A) be hired under section 213.3102(r) of title 5, Code of Federal Regulations; and

(B) be exempt from competitive service.

(2) COMPETITIVE SERVICE.—Upon satisfactory fulfillment of the service term under paragraph (1), an individual may be converted to a competitive service position without competition if the individual meets the requirements for that position.

(d) ELIGIBILITY.—The eligibility requirements for a scholarship under this section shall include that a scholarship applicant—

(1) be a citizen of the United States;

(2) be eligible to be granted a security clearance;

(3) maintain a grade point average of 3.2 or above on a 4.0 scale for undergraduate study or a 3.5 or above on a 4.0 scale for post-graduate study;

(4) demonstrate a commitment to a career in improving the security of the information infrastructure; and

(5) has demonstrated a level of proficiency in math or computer sciences.

(e) FAILURE TO COMPLETE SERVICE OBLIGATION.—

(1) IN GENERAL.—A scholarship recipient under this section shall be liable to the United States under paragraph (2) if the scholarship recipient—

(A) fails to maintain an acceptable level of academic standing in the educational institution in which the individual is enrolled, as determined by the Director;

(B) is dismissed from such educational institution for disciplinary reasons;

(C) withdraws from the program for which the award was made before the completion of such program;

(D) declares that the individual does not intend to fulfill the service obligation under this section;

(E) fails to fulfill the service obligation of the individual under this section; or

(F) loses a security clearance or becomes ineligible for a security clearance.

(2) REPAYMENT AMOUNTS.—

(A) LESS THAN 1 YEAR OF SERVICE.—If a circumstance under paragraph (1) occurs before the completion of 1 year of a service obligation under this section, the total amount of awards received by the individual under this section shall be repaid.

(B) ONE OR MORE YEARS OF SERVICE.—If a circumstance described in subparagraph (D) or (E) of paragraph (1) occurs after the completion of 1 year of a service obligation under this section, the total amount of scholarship awards received by the individual under this section, reduced by the ratio of the number of years of service completed divided by the number of years of service required, shall be repaid.

(f) EVALUATION AND REPORT.—The Director of the National Science Foundation shall—

(1) evaluate the success of recruiting individuals for scholarships under this section and of hiring and retaining those individuals in the public sector workforce, including the annual cost and an assessment of how the program actually improves the Federal workforce; and

(2) periodically report the findings under paragraph (1) to Congress.

(g) AUTHORIZATION OF APPROPRIATIONS.—From amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), the Director may use funds to carry out the requirements of this section for fiscal years 2012 through 2013.

SEC. 407. STUDY AND ANALYSIS OF CERTIFICATION AND TRAINING OF INFORMATION INFRASTRUCTURE PROFESSIONALS.

(a) STUDY.—The President shall enter into an agreement with the National Academies to conduct a comprehensive study of government, academic, and private-sector accreditation, training, and certification programs for personnel working in information infrastructure. The agreement shall require the National Academies to consult with sector coordinating councils and relevant governmental agencies, regulatory entities, and nongovernmental organizations in the course of the study.

(b) SCOPE.—The study shall include—

(1) an evaluation of the body of knowledge and various skills that specific categories of personnel working in information infrastructure should possess in order to secure information systems;

(2) an assessment of whether existing government, academic, and private-sector accreditation, training, and certification programs provide the body of knowledge and various skills described in paragraph (1);

(3) an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity talent, including barriers relating to compensation, the hiring process, job classification, and hiring flexibility; and

(4) an analysis of the sources and availability of cybersecurity talent, a comparison of the skills and expertise sought by the Federal Government and the private sector, an examination of the current and future capacity of United States institutions of higher

education, including community colleges, to provide current and future cybersecurity professionals, through education and training activities, with those skills sought by the Federal Government, State and local entities, and the private sector.

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the National Academies shall submit to the President and Congress a report on the results of the study. The report shall include—

(1) findings regarding the state of information infrastructure accreditation, training, and certification programs, including specific areas of deficiency and demonstrable progress; and

(2) recommendations for the improvement of information infrastructure accreditation, training, and certification programs.

SEC. 408. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

(a) IN GENERAL.—The Director of the National Institute of Standards and Technology, in coordination with appropriate Federal authorities, shall—

(1) as appropriate, ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to Congress a plan for ensuring such Federal agency coordination.

(b) CONSULTATION WITH THE PRIVATE SECTOR.—In carrying out the activities under subsection (a)(1), the Director shall ensure consultation with appropriate private sector stakeholders.

SEC. 409. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

The Director of the National Institute of Standards and Technology shall continue a program to support the development of technical standards, metrology, testbeds, and conformance criteria, taking into account appropriate user concerns—

(1) to improve interoperability among identity management technologies;

(2) to strengthen authentication methods of identity management systems;

(3) to improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols; and

(4) to improve the usability of identity management systems.

SEC. 410. FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY RESEARCH GRANT AREAS.—Section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking ''property.'' and inserting ''property;''; and

(3) by adding at the end the following:

''(J) secure fundamental protocols that are at the heart of inter-network communications and data exchange;

''(K) system security that addresses the building of secure systems from trusted and untrusted components;

''(L) monitoring and detection; and

''(M) resiliency and rapid recovery methods.''.

(b) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY GRANTS.—Section 4(a)(3) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(3)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(c) COMPUTER AND NETWORK SECURITY CENTERS.—Section 4(b)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7403(b)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(d) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—Section 5(a)(6) of the Cyber Security Research and Development Act (15 U.S.C. 7404(a)(6)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT GRANTS.—Section 5(b)(2) of the Cyber Security Research and Development Act (15 U.S.C. 7404(b)(2)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(f) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY RESEARCH.—Section 5(c)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7404(c)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

SA 2614. Mrs. HUTCHISON (for herself, Mr. MCCAIN, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin) submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012'' or ''SECURE IT''.

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

TITLE I—FACILITATING SHARING OF CYBER THREAT INFORMATION

SEC. 101. DEFINITIONS.

In this title:

(1) AGENCY.—The term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code.

(2) ANTITRUST LAWS.—The term ''antitrust laws''—

(A) has the meaning given the term in section 1(a) of the Clayton Act (15 U.S.C. 12(a));

(B) includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that section 5 of that Act applies to unfair methods of competition; and

(C) includes any State law that has the same intent and effect as the laws under subparagraphs (A) and (B).

(3) COUNTERMEASURE.—The term ''countermeasure'' means an automated or a manual action with defensive intent to mitigate cyber threats.

(4) CYBER THREAT INFORMATION.—The term ''cyber threat information'' means information that indicates or describes—

(A) a technical or operation vulnerability or a cyber threat mitigation measure;

(B) an action or operation to mitigate a cyber threat;

(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

(D) a method of defeating a technical control;

(E) a method of defeating an operational control;

(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

(G) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to inadvertently enable the defeat of a technical or operational control;

(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

(J) any combination of subparagraphs (A) through (I).

(5) CYBERSECURITY CENTER.—The term ''cybersecurity center'' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

(6) CYBERSECURITY SYSTEM.—The term ''cybersecurity system'' means a system designed or employed to ensure the integrity, confidentiality, or availability of, or to safeguard, a system or network, including measures intended to protect a system or network from—

(A) efforts to degrade, disrupt, or destroy such system or network; or

(B) theft or misappropriations of private or government information, intellectual property, or personally identifiable information.

(7) ENTITY.—

(A) IN GENERAL.—The term ''entity'' means any private entity, non-Federal government agency or department, or State, tribal, or local government agency or department (including an officer, employee, or agent thereof).

(B) INCLUSIONS.—The term ''entity'' includes a government agency or department (including an officer, employee, or agent thereof) of the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States.

(8) FEDERAL INFORMATION SYSTEM.—The term ''Federal information system'' means an information system of a Federal department or agency used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

(9) INFORMATION SECURITY.—The term ''information security'' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; or

(C) availability, by ensuring timely and reliable access to and use of information.

(10) INFORMATION SYSTEM.—The term ''information system'' has the meaning given the term in section 3502 of title 44, United States Code.

(11) LOCAL GOVERNMENT.—The term ''local government'' means any borough, city, county, parish, town, township, village, or other general purpose political subdivision of a State.

(12) MALICIOUS RECONNAISSANCE.—The term ''malicious reconnaissance'' means a method for actively probing or passively monitoring an information system for the purpose of discerning technical vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(13) OPERATIONAL CONTROL.—The term ''operational control'' means a security control for an information system that primarily is implemented and executed by people.

(14) OPERATIONAL VULNERABILITY.—The term ''operational vulnerability'' means any attribute of policy, process, or procedure that could enable or facilitate the defeat of an operational control.

(15) PRIVATE ENTITY.—The term ''private entity'' means any individual or any private group, organization, or corporation, including an officer, employee, or agent thereof.

(16) SIGNIFICANT CYBER INCIDENT.—The term ''significant cyber incident'' means a cyber incident resulting in, or an attempted cyber incident that, if successful, would have resulted in—

(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

(17) TECHNICAL CONTROL.—The term ''technical control'' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

(18) TECHNICAL VULNERABILITY.—The term ''technical vulnerability'' means any attribute of hardware or software that could enable or facilitate the defeat of a technical control.

(19) TRIBAL.—The term ''tribal'' has the meaning given the term ''Indian tribe'' in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

SEC. 102. AUTHORIZATION TO SHARE CYBER THREAT INFORMATION.

(a) VOLUNTARY DISCLOSURE.—

(1) PRIVATE ENTITIES.—Notwithstanding any other provision of law, a private entity may, for the purpose of preventing, investigating, or otherwise mitigating threats to information security, on its own networks, or as authorized by another entity, on such entity's networks, employ countermeasures and use cybersecurity systems in order to obtain, identify, or otherwise possess cyber threat information.

(2) ENTITIES.—Notwithstanding any other provision of law, an entity may disclose cyber threat information to—

(A) a cybersecurity center; or

(B) any other entity in order to assist with preventing, investigating, or otherwise mitigating threats to information security.

(3) INFORMATION SECURITY PROVIDERS.—If the cyber threat information described in paragraph (1) is obtained, identified, or otherwise possessed in the course of providing information security products or services under contract to another entity, that entity shall be given, at any time prior to disclosure of such information, a reasonable opportunity to authorize or prevent such disclosure, to request anonymization of such information, or to request that reasonable efforts be made to safeguard such information that identifies specific persons from unauthorized access or disclosure.

(b) SIGNIFICANT CYBER INCIDENTS INVOLVING FEDERAL INFORMATION SYSTEMS.—

(1) IN GENERAL.—An entity providing electronic communication services, remote computing services, or information security services to a Federal department or agency shall inform the Federal department or agency of a significant cyber incident involving the Federal information system of that Federal department or agency that—

(A) is directly known to the entity as a result of providing such services;

(B) is directly related to the provision of such services by the entity; and

(C) as determined by the entity, has impeded or will impede the performance of a critical mission of the Federal department or agency.

(2) ADVANCE COORDINATION.—A Federal department or agency receiving the services described in paragraph (1) shall coordinate in advance with an entity described in paragraph (1) to develop the parameters of any information that may be provided under paragraph (1), including clarification of the type of significant cyber incident that will impede the performance of a critical mission of the Federal department or agency.

(3) REPORT.—A Federal department or agency shall report information provided under this subsection to a cybersecurity center.

(4) CONSTRUCTION.—Any information provided to a cybersecurity center under paragraph (3) shall be treated in the same manner as information provided to a cybersecurity center under subsection (a).

(c) INFORMATION SHARED WITH OR PROVIDED TO A CYBERSECURITY CENTER.—Cyber threat information provided to a cybersecurity center under this section—

(1) may be disclosed to, retained by, and used by, consistent with otherwise applicable Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal government for a cybersecurity purpose, a national security purpose, or in order to prevent, investigate, or prosecute any of the offenses listed in section 2516 of title 18, United States Code, and such information shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under this paragraph;

(2) may, with the prior written consent of the entity submitting such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(3) shall be considered the commercial, financial, or proprietary information of the entity providing such information to the Federal government and any disclosure outside the Federal government may only be made upon the prior written consent by such entity and shall not constitute a waiver of

any applicable privilege or protection provided by law, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(4) shall be deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records;

(5) shall be, without discretion, withheld from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records;

(6) shall not be subject to the rules of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official;

(7) shall not, if subsequently provided to a State, tribal, or local government or government agency, otherwise be disclosed or distributed to any entity by such State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent; and

(8) shall not be directly used by any Federal, State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph.

(d) PROCEDURES RELATING TO INFORMATION SHARING WITH A CYBERSECURITY CENTER.—Not later than 60 days after the date of enactment of this Act, the heads of each department or agency containing a cybersecurity center shall jointly develop, promulgate, and submit to Congress procedures to ensure that cyber threat information shared with or provided to—

(1) a cybersecurity center under this section—

(A) may be submitted to a cybersecurity center by an entity, to the greatest extent possible, through a uniform, publicly available process or format that is easily accessible on the website of such cybersecurity center, and that includes the ability to provide relevant details about the cyber threat information and written consent to any subsequent disclosures authorized by this paragraph;

(B) shall immediately be further shared with each cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government;

(C) is handled by the Federal government in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title, and the Federal government may undertake efforts consistent with this subparagraph to limit the impact on privacy and civil liberties of the sharing of cyber threat information with the Federal government; and

(D) except as provided in this section, shall only be used, disclosed, or handled in accordance with the provisions of subsection (c); and

(2) a Federal agency or department under subsection (b) is provided immediately to a cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government.

(e) INFORMATION SHARED BETWEEN ENTITIES.—

(1) IN GENERAL.—An entity sharing cyber threat information with another entity under this title may restrict the use or sharing of such information by such other entity.

(2) FURTHER SHARING.—Cyber threat information shared by any entity with another entity under this title—

(A) shall only be further shared in accordance with any restrictions placed on the sharing of such information by the entity authorizing such sharing, such as appropriate anonymization of such information; and

(B) may not be used by any entity to gain an unfair competitive advantage to the detriment of the entity authorizing the sharing of such information, except that the conduct described in paragraph (3) shall not constitute unfair competitive conduct.

(3) INFORMATION SHARED WITH STATE, TRIBAL, OR LOCAL GOVERNMENT OR GOVERNMENT AGENCY.—Cyber threat information shared with a State, tribal, or local government or government agency under this title—

(A) may, with the prior written consent of the entity sharing such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent;

(B) shall be deemed voluntarily shared information and exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records;

(C) shall not be disclosed or distributed to any entity by the State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent; and

(D) shall not be directly used by any State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this subparagraph.

(4) ANTITRUST EXEMPTION.—The exchange or provision of cyber threat information or assistance between 2 or more private entities under this title shall not be considered a violation of any provision of antitrust laws if exchanged or provided in order to assist with—

(A) facilitating the prevention, investigation, or mitigation of threats to information security; or

(B) communicating or disclosing of cyber threat information to help prevent, investigate or otherwise mitigate the effects of a threat to information security.

(5) NO RIGHT OR BENEFIT.—The provision of cyber threat information to an entity under this section shall not create a right or a benefit to similar information by such entity or any other entity.

(f) FEDERAL PREEMPTION.—

(1) IN GENERAL.—This section supersedes any statute or other law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this section.

(2) STATE LAW ENFORCEMENT.—Nothing in this section shall be construed to supersede any statute or other law of a State or political subdivision of a State concerning the use of authorized law enforcement techniques.

(3) PUBLIC DISCLOSURE.—No information shared with or provided to a State, tribal, or local government or government agency pursuant to this section shall be made publicly available pursuant to any State, tribal, or local law requiring disclosure of information or records.

(g) CIVIL AND CRIMINAL LIABILITY.—

(1) GENERAL PROTECTIONS.—

(A) PRIVATE ENTITIES.—No cause of action shall lie or be maintained in any court against any private entity for—

(i) the use of countermeasures and cybersecurity systems as authorized by this title;

(ii) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(iii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such private entity.

(B) ENTITIES.—No cause of action shall lie or be maintained in any court against any entity for—

(i) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(ii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such entity.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed as creating any immunity against, or otherwise affecting, any action brought by the Federal government, or any agency or department thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, and use of classified information.

(h) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this section shall be construed to limit or prohibit otherwise lawful disclosures of communications, records, or other information by a private entity to any other governmental or private entity not covered under this section.

(i) WHISTLEBLOWER PROTECTION.—Nothing in this Act shall be construed to preempt or preclude any employee from exercising rights currently provided under any whistleblower law, rule, or regulation.

(j) RELATIONSHIP TO OTHER LAWS.—The submission of cyber threat information under this section to a cybersecurity center shall not affect any requirement under any other provision of law for an entity to provide information to the Federal government.

SEC. 103. INFORMATION SHARING BY THE FEDERAL GOVERNMENT.

(a) CLASSIFIED INFORMATION.—

(1) PROCEDURES.—Consistent with the protection of intelligence sources and methods, and as otherwise determined appropriate, the Director of National Intelligence and the Secretary of Defense, in consultation with the heads of the appropriate Federal departments or agencies, shall develop and promulgate procedures to facilitate and promote—

(A) the immediate sharing, through the cybersecurity centers, of classified cyber threat information in the possession of the Federal government with appropriately cleared representatives of any appropriate entity; and

(B) the declassification and immediate sharing, through the cybersecurity centers, with any entity or, if appropriate, public availability of cyber threat information in the possession of the Federal government;

(2) HANDLING OF CLASSIFIED INFORMATION.—The procedures developed under paragraph

(1) shall ensure that each entity receiving classified cyber threat information pursuant to this section has acknowledged in writing the ongoing obligation to comply with all laws, executive orders, and procedures concerning the appropriate handling, disclosure, or use of classified information.

(b) UNCLASSIFIED CYBER THREAT INFORMATION.—The heads of each department or agency containing a cybersecurity center shall jointly develop and promulgate procedures that ensure that, consistent with the provisions of this section, unclassified, including controlled unclassified, cyber threat information in the possession of the Federal government—

(1) is shared, through the cybersecurity centers, in an immediate and adequate manner with appropriate entities; and

(2) if appropriate, is made publicly available.

(c) DEVELOPMENT OF PROCEDURES.—

(1) IN GENERAL.—The procedures developed under this section shall incorporate, to the greatest extent possible, existing processes utilized by sector specific information sharing and analysis centers.

(2) COORDINATION WITH ENTITIES.—In developing the procedures required under this section, the Director of National Intelligence and the heads of each department or agency containing a cybersecurity center shall coordinate with appropriate entities to ensure that protocols are implemented that will facilitate and promote the sharing of cyber threat information by the Federal government.

(d) ADDITIONAL RESPONSIBILITIES OF CYBERSECURITY CENTERS.—Consistent with section 102, a cybersecurity center shall—

(1) facilitate information sharing, interaction, and collaboration among and between cybersecurity centers and—

(A) other Federal entities;

(B) any entity; and

(C) international partners, in consultation with the Secretary of State;

(2) disseminate timely and actionable cybersecurity threat, vulnerability, mitigation, and warning information, including alerts, advisories, indicators, signatures, and mitigation and response measures, to improve the security and protection of information systems; and

(3) coordinate with other Federal entities, as appropriate, to integrate information from across the Federal government to provide situational awareness of the cybersecurity posture of the United States.

(e) SHARING WITHIN THE FEDERAL GOVERNMENT.—The heads of appropriate Federal departments and agencies shall ensure that cyber threat information in the possession of such Federal departments or agencies that relates to the prevention, investigation, or mitigation of threats to information security across the Federal government is shared effectively with the cybersecurity centers.

(f) SUBMISSION TO CONGRESS.—Not later than 60 days after the date of enactment of this Act, the Director of National Intelligence, in coordination with the appropriate head of a department or an agency containing a cybersecurity center, shall submit the procedures required by this section to Congress.

SEC. 104. CONSTRUCTION.

(a) INFORMATION SHARING RELATIONSHIPS.—Nothing in this title shall be construed—

(1) to limit or modify an existing information sharing relationship;

(2) to prohibit a new information sharing relationship;

(3) to require a new information sharing relationship between any entity and the Federal government, except as specified under section 102(b); or

(4) to modify the authority of a department or agency of the Federal government to protect sources and methods and the national security of the United States.

(b) ANTI-TASKING RESTRICTION.—Nothing in this title shall be construed to permit the Federal government—

(1) to require an entity to share information with the Federal government, except as expressly provided under section 102(b); or

(2) to condition the sharing of cyber threat information with an entity on such entity's provision of cyber threat information to the Federal government.

(c) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this title shall be construed to subject any entity to liability for choosing not to engage in the voluntary activities authorized under this title.

(d) USE AND RETENTION OF INFORMATION.—Nothing in this title shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal government to retain or use any information shared under section 102 for any use other than a use permitted under subsection 102(c)(1).

(e) NO NEW FUNDING.—An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 105. REPORT ON IMPLEMENTATION.

(a) CONTENT OF REPORT.—Not later than 1 year after the date of enactment of this Act, and biennially thereafter, the heads of each department or agency containing a cybersecurity center shall jointly submit, in coordination with the privacy and civil liberties officials of such departments or agencies and the Privacy and Civil Liberties Oversight Board, a detailed report to Congress concerning the implementation of this title, including—

(1) an assessment of the sufficiency of the procedures developed under section 103 of this Act in ensuring that cyber threat information in the possession of the Federal government is provided in an immediate and adequate manner to appropriate entities or, if appropriate, is made publicly available;

(2) an assessment of whether information has been appropriately classified and an accounting of the number of security clearances authorized by the Federal government for purposes of this title;

(3) a review of the type of cyber threat information shared with a cybersecurity center under section 102 of this Act, including whether such information meets the definition of cyber threat information under section 101, the degree to which such information may impact the privacy and civil liberties of individuals, any appropriate metrics to determine any impact of the sharing of such information with the Federal government on privacy and civil liberties, and the adequacy of any steps taken to reduce such impact;

(4) a review of actions taken by the Federal government based on information provided to a cybersecurity center under section 102 of this Act, including the appropriateness of any subsequent use under section 102(c)(1) of this Act and whether there was inappropriate stovepiping within the Federal government of any such information;

(5) a description of any violations of the requirements of this title by the Federal government;

(6) a classified list of entities that received classified information from the Federal government under section 103 of this Act and a description of any indication that such information may not have been appropriately handled;

(7) a summary of any breach of information security, if known, attributable to a specific failure by any entity or the Federal government to act on cyber threat information in the possession of such entity or the Federal government that resulted in substantial economic harm or injury to a specific entity or the Federal government; and

(8) any recommendation for improvements or modifications to the authorities under this title.

(b) FORM OF REPORT.—The report under subsection (a) shall be submitted in unclassified form, but shall include a classified annex.

SEC. 106. INSPECTOR GENERAL REVIEW.

(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency are authorized to review compliance by the cybersecurity centers, and by any Federal department or agency receiving cyber threat information from such cybersecurity centers, with the procedures required under section 102 of this Act.

(b) SCOPE OF REVIEW.—The review under subsection (a) shall consider whether the Federal government has handled such cyber threat information in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title.

(c) REPORT TO CONGRESS.—Each review conducted under this section shall be provided to Congress not later than 30 days after the date of completion of the review.

SEC. 107. TECHNICAL AMENDMENTS.

Section 552(b) of title 5, United States Code, is amended—

(1) in paragraph (8), by striking ''or'';

(2) in paragraph (9), by striking ''wells.'' and inserting ''wells; or''; and

(3) by adding at the end the following:

''(10) information shared with or provided to a cybersecurity center under section 102 of title I of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012.''.

SEC. 108. ACCESS TO CLASSIFIED INFORMATION.

(a) AUTHORIZATION REQUIRED.—No person shall be provided with access to classified information (as defined in section 6.1 of Executive Order 13526 (50 U.S.C. 435 note; relating to classified national security information)) relating to cyber security threats or cyber security vulnerabilities under this title without the appropriate security clearances.

(b) SECURITY CLEARANCES.—The appropriate Federal agencies or departments shall, consistent with applicable procedures and requirements, and if otherwise deemed appropriate, assist an individual in timely obtaining an appropriate security clearance where such individual has been determined to be eligible for such clearance and has a need-to-know (as defined in section 6.1 of that Executive Order) classified information to carry out this title.

TITLE II—COORDINATION OF FEDERAL INFORMATION SECURITY POLICY

SEC. 201. COORDINATION OF FEDERAL INFORMATION SECURITY POLICY.

(a) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by striking subchapters II and III and inserting the following:

''SUBCHAPTER II—INFORMATION SECURITY

''§ 3551. Purposes

''The purposes of this subchapter are—

''(1) to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

''(2) to recognize the highly networked nature of the current Federal computing environment and provide effective government-

wide management of policies, directives, standards, and guidelines, as well as effective and nimble oversight of and response to information security risks, including coordination of information security efforts throughout the Federal civilian, national security, and law enforcement communities;

''(3) to provide for development and maintenance of controls required to protect agency information and information systems and contribute to the overall improvement of agency information security posture;

''(4) to provide for the development of tools and methods to assess and respond to real-time situational risk for Federal information system operations and assets; and

''(5) to provide a mechanism for improving agency information security programs through continuous monitoring of agency information systems and streamlined reporting requirements rather than overly prescriptive manual reporting.

''§ 3552. Definitions

''In this subchapter:

''(1) ADEQUATE SECURITY.—The term 'adequate security' means security commensurate with the risk and magnitude of the harm resulting from the unauthorized access to or loss, misuse, destruction, or modification of information.

''(2) AGENCY.—The term 'agency' has the meaning given the term in section 3502 of title 44.

''(3) CYBERSECURITY CENTER.—The term 'cybersecurity center' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

''(4) CYBER THREAT INFORMATION.—The term 'cyber threat information' means information that indicates or describes—

''(A) a technical or operation vulnerability or a cyber threat mitigation measure;

''(B) an action or operation to mitigate a cyber threat;

''(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

''(D) a method of defeating a technical control;

''(E) a method of defeating an operational control;

''(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

''(G) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to inadvertently enable the defeat of a technical or operational control;

''(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

''(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

''(J) any combination of subparagraphs (A) through (I).

''(5) DIRECTOR.—The term 'Director' means the Director of the Office of Management and Budget unless otherwise specified.

''(6) ENVIRONMENT OF OPERATION.—The term 'environment of operation' means the information system and environment in which those systems operate, including changing threats, vulnerabilities, technologies, and missions and business practices.

''(7) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

''(8) INCIDENT.—The term 'incident' means an occurrence that—

''(A) actually or imminently jeopardizes the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores, or transmits; or

''(B) constitutes a violation of law or an imminent threat of violation of a law, a security policy, a security procedure, or an acceptable use policy.

''(9) INFORMATION RESOURCES.—The term 'information resources' has the meaning given the term in section 3502 of title 44.

''(10) INFORMATION SECURITY.—The term 'information security' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

''(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

''(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; or

''(C) availability, by ensuring timely and reliable access to and use of information.

''(11) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44.

''(12) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given the term in section 11101 of title 40.

''(13) MALICIOUS RECONNAISSANCE.—The term 'malicious reconnaissance' means a method for actively probing or passively monitoring an information system for the purpose of discerning technical vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

''(14) NATIONAL SECURITY SYSTEM.—

''(A) IN GENERAL.—The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

''(i) the function, operation, or use of which—

''(I) involves intelligence activities;

''(II) involves cryptologic activities related to national security;

''(III) involves command and control of military forces;

''(IV) involves equipment that is an integral part of a weapon or weapons system; or

''(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

''(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

''(B) LIMITATION.—Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

''(15) OPERATIONAL CONTROL.—The term 'operational control' means a security control for an information system that primarily is implemented and executed by people.

''(16) PERSON.—The term 'person' has the meaning given the term in section 3502 of title 44.

''(17) SECRETARY.—The term 'Secretary' means the Secretary of Commerce unless otherwise specified.

''(18) SECURITY CONTROL.—The term 'security control' means the management, operational, and technical controls, including safeguards or countermeasures, prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

''(19) SIGNIFICANT CYBER INCIDENT.—The term 'significant cyber incident' means a cyber incident resulting in, or an attempted cyber incident that, if successful, would have resulted in—

''(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

''(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

''(20) TECHNICAL CONTROL.—The term 'technical control' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

''§ 3553. Federal information security authority and coordination

''(a) IN GENERAL.—The Secretary, in consultation with the Secretary of Homeland Security, shall—

''(1) issue compulsory and binding policies and directives governing agency information security operations, and require implementation of such policies and directives, including—

''(A) policies and directives consistent with the standards and guidelines promulgated under section 11331 of title 40 to identify and provide information security protections prioritized and commensurate with the risk and impact resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by or on behalf of an agency; or

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(B) minimum operational requirements for Federal Government to protect agency information systems and provide common situational awareness across all agency information systems;

''(C) reporting requirements, consistent with relevant law, regarding information security incidents and cyber threat information;

''(D) requirements for agencywide information security programs;

''(E) performance requirements and metrics for the security of agency information systems;

''(F) training requirements to ensure that agencies are able to fully and timely comply with the policies and directives issued by the Secretary under this subchapter;

''(G) training requirements regarding privacy, civil rights, and civil liberties, and information oversight for agency information security personnel;

''(H) requirements for the annual reports to the Secretary under section 3554(d);

''(I) any other information security operations or information security requirements as determined by the Secretary in coordination with relevant agency heads; and

''(J) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

''(2) review the agencywide information security programs under section 3554; and

''(3) designate an individual or an entity at each cybersecurity center, among other responsibilities—

''(A) to receive reports and information about information security incidents, cyber threat information, and deterioration of security control affecting agency information systems; and

''(B) to act on or share the information under subparagraph (A) in accordance with this subchapter.

''(b) CONSIDERATIONS.—When issuing policies and directives under subsection (a), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology under section 11331 of title 40.

''(c) LIMITATION OF AUTHORITY.—The authorities of the Secretary under this section shall not apply to national security systems. Information security policies, directives, standards and guidelines for national security systems shall be overseen as directed by the President and, in accordance with that direction, carried out under the authority of the heads of agencies that operate or exercise authority over such national security systems.

''(d) STATUTORY CONSTRUCTION.—Nothing in this subchapter shall be construed to alter or amend any law regarding the authority of any head of an agency over such agency.

''§ 3554. Agency responsibilities

''(a) IN GENERAL.—The head of each agency shall—

''(1) be responsible for—

''(A) complying with the policies and directives issued under section 3553;

''(B) providing information security protections commensurate with the risk resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by the agency or by a contractor of an agency or other organization on behalf of an agency; and

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(C) complying with the requirements of this subchapter, including—

''(i) information security standards and guidelines promulgated under section 11331 of title 40;

''(ii) for any national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued as directed by the President; and

''(iii) for any non-national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued under section 3553;

''(D) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

''(E) reporting and sharing, for an agency operating or exercising control of a national security system, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for national security systems issued as directed by the President; and

''(F) reporting and sharing, for those agencies operating or exercising control of non-national security systems, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for non-national security systems as prescribed under section 3553(a), including information to assist the entity designated under section 3555(a) with the ongoing security analysis under section 3555;

''(2) ensure that each senior agency official provides information security for the information and information systems that support the operations and assets under the senior agency official's control, including by—

''(A) assessing the risk and impact that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

''(B) determining the level of information security appropriate to protect such information and information systems in accordance with policies and directives issued under section 3553(a), and standards and guidelines promulgated under section 11331 of title 40 for information security classifications and related requirements;

''(C) implementing policies, procedures, and capabilities to reduce risks to an acceptable level in a cost-effective manner;

''(D) actively monitoring the effective implementation of information security controls and techniques; and

''(E) reporting information about information security incidents, cyber threat information, and deterioration of security controls in a timely and adequate manner to the entity designated under section 3553(a)(3) in accordance with paragraph (1);

''(3) assess and maintain the resiliency of information technology systems critical to agency mission and operations;

''(4) designate the agency Inspector General (or an independent entity selected in consultation with the Director and the Council of Inspectors General on Integrity and Efficiency if the agency does not have an Inspector General) to conduct the annual independent evaluation required under section 3556, and allow the agency Inspector General to contract with an independent entity to perform such evaluation;

''(5) delegate to the Chief Information Officer or equivalent (or to a senior agency official who reports to the Chief Information Officer or equivalent)—

''(A) the authority and primary responsibility to implement an agencywide information security program; and

''(B) the authority to provide information security for the information collected and maintained by the agency (or by a contractor, other agency, or other source on behalf of the agency) and for the information systems that support the operations, assets, and mission of the agency (including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency);

''(6) delegate to the appropriate agency official (who is responsible for a particular agency system or subsystem) the responsibility to ensure and enforce compliance with all requirements of the agency's agencywide information security program in coordination with the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5);

''(7) ensure that an agency has trained personnel who have obtained any necessary security clearances to permit them to assist the agency in complying with this subchapter;

''(8) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5), in coordination with other senior agency officials, reports to the agency head on the effectiveness of the agencywide information security program, including the progress of any remedial actions; and

''(9) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5) has the necessary qualifications to administer the functions described in this subchapter and has information security duties as a primary duty of that official.

''(b) CHIEF INFORMATION OFFICERS.—Each Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under subsection (a)(5) shall—

''(1) establish and maintain an enterprise security operations capability that on a continuous basis—

''(A) detects, reports, contains, mitigates, and responds to information security incidents that impair adequate security of the agency's information or information system in a timely manner and in accordance with the policies and directives under section 3553; and

''(B) reports any information security incident under subparagraph (A) to the entity designated under section 3555;

''(2) develop, maintain, and oversee an agencywide information security program;

''(3) develop, maintain, and oversee information security policies, procedures, and control techniques to address applicable requirements, including requirements under section 3553 of this title and section 11331 of title 40; and

''(4) train and oversee the agency personnel who have significant responsibility for information security with respect to that responsibility.

''(c) AGENCYWIDE INFORMATION SECURITY PROGRAMS.—

''(1) IN GENERAL.—Each agencywide information security program under subsection (b)(2) shall include—

''(A) relevant security risk assessments, including technical assessments and others related to the acquisition process;

''(B) security testing commensurate with risk and impact;

''(C) mitigation of deterioration of security controls commensurate with risk and impact;

''(D) risk-based continuous monitoring and threat assessment of the operational status and security of agency information systems to enable evaluation of the effectiveness of and compliance with information security policies, procedures, and practices, including a relevant and appropriate selection of security controls of information systems identified in the inventory under section 3505(c);

''(E) operation of appropriate technical capabilities in order to detect, mitigate, report, and respond to information security incidents, cyber threat information, and deterioration of security controls in a manner that is consistent with the policies and directives under section 3553, including—

''(i) mitigating risks associated with such information security incidents;

''(ii) notifying and consulting with the entity designated under section 3555; and

''(iii) notifying and consulting with, as appropriate—

''(I) law enforcement and the relevant Office of the Inspector General; and

''(II) any other entity, in accordance with law and as directed by the President;

''(F) a process to ensure that remedial action is taken to address any deficiencies in the information security policies, procedures, and practices of the agency; and

''(G) a plan and procedures to ensure the continuity of operations for information systems that support the operations and assets of the agency.

''(2) RISK MANAGEMENT STRATEGIES.—Each agencywide information security program under subsection (b)(2) shall include the development and maintenance of a risk management strategy for information security. The risk management strategy shall include—

''(A) consideration of information security incidents, cyber threat information, and deterioration of security controls; and

''(B) consideration of the consequences that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency;

''(3) POLICIES AND PROCEDURES.—Each agencywide information security program under subsection (b)(2) shall include policies and procedures that—

''(A) are based on the risk management strategy under paragraph (2);

''(B) reduce information security risks to an acceptable level in a cost-effective manner;

''(C) ensure that cost-effective and adequate information security is addressed as part of the acquisition and ongoing management of each agency information system; and

''(D) ensure compliance with—

''(i) this subchapter; and

''(ii) any other applicable requirements.

''(4) TRAINING REQUIREMENTS.—Each agencywide information security program under subsection (b)(2) shall include information security, privacy, civil rights, civil liberties, and information oversight training that meets any applicable requirements under section 3553. The training shall inform each information security personnel that has access to agency information systems (including contractors and other users of information systems that support the operations and assets of the agency) of—

''(A) the information security risks associated with the information security personnel's activities; and

''(B) the individual's responsibility to comply with the agency policies and procedures that reduce the risks under subparagraph (A).

''(d) ANNUAL REPORT.—Each agency shall submit a report annually to the Secretary of Homeland Security on its agencywide information security program and information systems.

''§ 3555. Multiagency ongoing threat assessment

''(a) IMPLEMENTATION.—The Director of the Office of Management and Budget, in coordination with the Secretary of Homeland Security, shall designate an entity to implement ongoing security analysis concerning agency information systems—

''(1) based on cyber threat information;

''(2) based on agency information system and environment of operation changes, including—

''(A) an ongoing evaluation of the information system security controls; and

''(B) the security state, risk level, and environment of operation of an agency information system, including—

''(i) a change in risk level due to a new cyber threat;

''(ii) a change resulting from a new technology;

''(iii) a change resulting from the agency's mission; and

''(iv) a change resulting from the business practice; and

''(3) using automated processes to the maximum extent possible—

''(A) to increase information system security;

''(B) to reduce paper-based reporting requirements; and

''(C) to maintain timely and actionable knowledge of the state of the information system security.

''(b) STANDARDS.—The National Institute of Standards and Technology may promulgate standards, in coordination with the Secretary of Homeland Security, to assist an agency with its duties under this section.

''(c) COMPLIANCE.—The head of each appropriate department and agency shall be responsible for ensuring compliance and implementing necessary procedures to comply with this section. The head of each appropriate department and agency, in consultation with the Director of the Office of Management and Budget and the Secretary of Homeland Security, shall—

''(1) monitor compliance under this section;

''(2) develop a timeline and implement for the department or agency—

''(A) adoption of any technology, system, or method that facilitates continuous monitoring and threat assessments of an agency information system;

''(B) adoption or updating of any technology, system, or method that prevents, detects, or remediates a significant cyber incident to a Federal information system of the department or agency that has impeded, or is reasonably likely to impede, the performance of a critical mission of the department or agency; and

''(C) adoption of any technology, system, or method that satisfies a requirement under this section.

''(d) LIMITATION OF AUTHORITY.—The authorities of the Director of the Office of Management and Budget and of the Secretary of Homeland Security under this section shall not apply to national security systems.

''(e) REPORT.—Not later than 6 months after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Government Accountability Office shall issue a report evaluating each agency's status toward implementing this section.

''§ 3556. Independent evaluations

''(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency, in consultation with the Director and the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense, shall issue and maintain criteria for the timely, cost-effective, risk-based, and independent evaluation of each agencywide information security program (and practices) to determine the effectiveness of the agencywide information security program (and practices). The criteria shall include measures to assess any conflicts of interest in the performance of the evaluation and whether the agencywide information security program includes appropriate safeguards against disclosure of information where such disclosure may adversely affect information security.

''(b) ANNUAL INDEPENDENT EVALUATIONS.—Each agency shall perform an annual independent evaluation of its agencywide information security program (and practices) in accordance with the criteria under subsection (a).

''(c) DISTRIBUTION OF REPORTS.—Not later than 30 days after receiving an independent evaluation under subsection (b), each agency head shall transmit a copy of the independent evaluation to the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense.

''(d) NATIONAL SECURITY SYSTEMS.—Evaluations involving national security systems shall be conducted as directed by President.

''§ 3557. National security systems.

''The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

''(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system; and

''(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President.''.

(b) SAVINGS PROVISIONS.—

(1) POLICY AND COMPLIANCE GUIDANCE.—Policy and compliance guidance issued by the Director before the date of enactment of this Act under section 3543(a)(1) of title 44, United States Code (as in effect on the day before the date of enactment of this Act), shall continue in effect, according to its terms, until modified, terminated, superseded, or repealed pursuant to section 3553(a)(1) of title 44, United States Code.

(2) STANDARDS AND GUIDELINES.—Standards and guidelines issued by the Secretary of Commerce or by the Director before the date of enactment of this Act under section 11331(a)(1) of title 40, United States Code, (as in effect on the day before the date of enactment of this Act) shall continue in effect, according to their terms, until modified, terminated, superseded, or repealed pursuant to section 11331(a)(1) of title 40, United States Code, as amended by this Act.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) CHAPTER ANALYSIS.—The chapter analysis for chapter 35 of title 44, United States Code, is amended—

(A) by striking the items relating to sections 3531 through 3538;

(B) by striking the items relating to sections 3541 through 3549; and

(C) by inserting the following:

''3551. Purposes.
''3552. Definitions.
''3553. Federal information security authority and coordination.
''3554. Agency responsibilities.
''3555. Multiagency ongoing threat assessment.
''3556. Independent evaluations.
''3557. National security systems.''.

(2) OTHER REFERENCES.—

(A) Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(1)(A)) is amended by striking ''section 3532(3)'' and inserting ''section 3552''.

(B) Section 2222(j)(5) of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(C) Section 2223(c)(3) of title 10, United States Code, is amended, by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(D) Section 2315 of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(E) Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended—

(i) in subsection (a)(2), by striking ''section 3532(b)(2)'' and inserting ''section 3552'';

(ii) in subsection (c)(3), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iii) in subsection (d)(1), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iv) in subsection (d)(8) by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(v) in subsection (d)(8), by striking ''submitted to the Director'' and inserting ''submitted to the Secretary'';

(vi) in subsection (e)(2), by striking ''section 3532(1) of such title'' and inserting ''section 3552 of title 44''; and

(vii) in subsection (e)(5), by striking ''section 3532(b)(2) of such title'' and inserting ''section 3552 of title 44''.

(F) Section 8(d)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7406(d)(1)) is amended by striking ''section 3534(b)'' and inserting ''section 3554(b)(2)''.

SEC. 202. MANAGEMENT OF INFORMATION TECHNOLOGY.

(a) IN GENERAL.—Section 11331 of title 40, United States Code, is amended to read as follows:

''§ 11331. Responsibilities for Federal information systems standards

''(a) STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO PRESCRIBE.—Except as provided under paragraph (2), the Secretary of Commerce shall prescribe standards and guidelines pertaining to Federal information systems—

''(A) in consultation with the Secretary of Homeland Security; and

''(B) on the basis of standards and guidelines developed by the National Institute of Standards and Technology under paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)(2) and (a)(3)).

''(2) NATIONAL SECURITY SYSTEMS.—Standards and guidelines for national security systems shall be developed, prescribed, enforced, and overseen as otherwise authorized by law and as directed by the President.

''(b) MANDATORY STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO MAKE MANDATORY STANDARDS AND GUIDELINES.—The Secretary of Commerce shall make standards and guidelines under subsection (a)(1) compulsory and binding to the extent determined necessary by the Secretary of Commerce to improve the efficiency of operation or security of Federal information systems.

''(2) REQUIRED MANDATORY STANDARDS AND GUIDELINES.—

''(A) IN GENERAL.—Standards and guidelines under subsection (a)(1) shall include information security standards that—

''(i) provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)); and

''(ii) are otherwise necessary to improve the security of Federal information and information systems.

''(B) BINDING EFFECT.—Information security standards under subparagraph (A) shall be compulsory and binding.

''(c) EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary of Commerce shall exercise the authority conferred by this section subject to direction by the President and in coordination with the Director.

''(d) APPLICATION OF MORE STRINGENT STANDARDS AND GUIDELINES.—The head of an executive agency may employ standards for the cost-effective information security for information systems within or under the supervision of that agency that are more stringent than the standards and guidelines the Secretary of Commerce prescribes under this section if the more stringent standards and guidelines—

''(1) contain at least the applicable standards and guidelines made compulsory and binding by the Secretary of Commerce; and

''(2) are otherwise consistent with the policies, directives, and implementation memoranda issued under section 3553(a) of title 44.

''(e) DECISIONS ON PROMULGATION OF STANDARDS AND GUIDELINES.—The decision by the Secretary of Commerce regarding the promulgation of any standard or guideline under this section shall occur not later than 6 months after the date of submission of the proposed standard to the Secretary of Commerce by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

''(f) NOTICE AND COMMENT.—A decision by the Secretary of Commerce to significantly modify, or not promulgate, a proposed standard submitted to the Secretary by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) shall be made after the public is given an opportunity to comment on the Secretary's proposed decision.

''(g) DEFINITIONS.—In this section:

''(1) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' has the meaning given the term in section 3552 of title 44.

''(2) INFORMATION SECURITY.—The term 'information security' has the meaning given the term in section 3552 of title 44.

''(3) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given the term in section 3552 of title 44.''.

SEC. 203. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 204. TECHNICAL AND CONFORMING AMENDMENTS.

Section 21(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4(b)) is amended—

(1) in paragraph (2), by striking ''and the Director of the Office of Management and Budget'' and inserting '', the Secretary of Commerce, and the Secretary of Homeland Security''; and

(2) in paragraph (3), by inserting '', the Secretary of Homeland Security,'' after ''the Secretary of Commerce''.

SEC. 205. CLARIFICATION OF AUTHORITIES.

Nothing in this title shall be construed to convey any new regulatory authority to any government entity implementing or complying with any provision of this title.

TITLE III—CRIMINAL PENALTIES

SEC. 301. PENALTIES FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030(c) of title 18, United States Code, is amended to read as follows:

''(c) The punishment for an offense under subsection (a) or (b) of this section is—

''(1) a fine under this title or imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(1) of this section;

''(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than 3 years, or both, in the case of an offense under subsection (a)(2); or

''(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2) of this section, if—

''(i) the offense was committed for purposes of commercial advantage or private financial gain;

''(ii) the offense was committed in the furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States, or of any State; or

''(iii) the value of the information obtained, or that would have been obtained if the offense was completed, exceeds $5,000;

''(3) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(3) of this section;

''(4) a fine under this title or imprisonment of not more than 20 years, or both, in the case of an offense under subsection (a)(4) of this section;

''(5)(A) except as provided in subparagraph (C), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A) of this section, if the offense caused—

''(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

''(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

''(iii) physical injury to any person;

''(iv) a threat to public health or safety;

''(v) damage affecting a computer used by, or on behalf of, an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

''(vi) damage affecting 10 or more protected computers during any 1-year period;

''(B) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(B), if the offense caused a harm provided in clause (i) through (vi) of subparagraph (A) of this subsection;

''(C) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both;

''(D) a fine under this title, imprisonment for not more than 10 years, or both, for any other offense under subsection (a)(5);

''(E) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(6) of this section; or

''(F) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(7) of this section.''.

SEC. 302. TRAFFICKING IN PASSWORDS.

Section 1030(a)(6) of title 18, United States Code, is amended to read as follows:

''(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information or means of access through which a protected computer (as defined in subparagraphs (A) and (B) of subsection (e)(2)) may be accessed without authorization.''.

SEC. 303. CONSPIRACY AND ATTEMPTED COMPUTER FRAUD OFFENSES.

Section 1030(b) of title 18, United States Code, is amended by inserting ''as if for the completed offense'' after ''punished as provided''.

SEC. 304. CRIMINAL AND CIVIL FORFEITURE FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030 of title 18, United States Code, is amended by striking subsections (i) and (j) and inserting the following:

''(i) CRIMINAL FORFEITURE.—

''(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

''(A) such persons interest in any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of such violation; and

''(B) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of such violation.

''(2) The criminal forfeiture of property under this subsection, including any seizure and disposition of the property, and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

''(j) CIVIL FORFEITURE.—

''(1) The following shall be subject to forfeiture to the United States and no property right, real or personal, shall exist in them:

''(A) Any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of any violation of this section, or a conspiracy to violate this section.

''(B) Any property, real or personal, constituting or derived from any gross proceeds obtained directly or indirectly, or any property traceable to such property, as a result of the commission of any violation of this section, or a conspiracy to violate this section.

''(2) Seizures and forfeitures under this subsection shall be governed by the provisions in chapter 46 relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents and other persons as may be designated for that purpose by the Secretary of Homeland Security or the Attorney General.''.

SEC. 305. DAMAGE TO CRITICAL INFRASTRUCTURE COMPUTERS.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

''§ 1030A. Aggravated damage to a critical infrastructure computer

''(a) DEFINITIONS.—In this section—

''(1) the term 'computer' has the meaning given the term in section 1030;

''(2) the term 'critical infrastructure computer' means a computer that manages or controls systems or assets vital to national defense, national security, national economic security, public health or safety, or any combination of those matters, whether publicly or privately owned or operated, including—

''(A) oil and gas production, storage, conversion, and delivery systems;

''(B) water supply systems;

''(C) telecommunication networks;

''(D) electrical power generation and delivery systems;

''(E) finance and banking systems;

''(F) emergency services;

''(G) transportation systems and services; and

''(H) government operations that provide essential services to the public; and

''(3) the term 'damage' has the meaning given the term in section 1030.

''(b) OFFENSE.—It shall be unlawful, during and in relation to a felony violation of section 1030, to knowingly cause or attempt to cause damage to a critical infrastructure computer if the damage results in (or, in the case of an attempt, if completed, would have resulted in) the substantial impairment—

''(1) of the operation of the critical infrastructure computer; or

''(2) of the critical infrastructure associated with the computer.

''(c) PENALTY.—Any person who violates subsection (b) shall be—

''(1) fined under this title;

''(2) imprisoned for not less than 3 years but not more than 20 years; or

''(3) penalized under paragraphs (1) and (2).

''(d) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

''(1) a court shall not place on probation any person convicted of a violation of this section;

''(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment, including any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for a felony violation of section 1030;

''(3) in determining any term of imprisonment to be imposed for a felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The chapter analysis for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

''1030A. Aggravated damage to a critical infrastructure computer.''.

SEC. 306. LIMITATION ON ACTIONS INVOLVING UNAUTHORIZED USE.

Section 1030(e)(6) of title 18, United States Code, is amended by striking ''alter;'' and inserting ''alter, but does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized;''.

SEC. 307. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

TITLE IV—CYBERSECURITY RESEARCH AND DEVELOPMENT

SEC. 401. NATIONAL HIGH-PERFORMANCE COMPUTING PROGRAM PLANNING AND COORDINATION.

(a) GOALS AND PRIORITIES.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(d) GOALS AND PRIORITIES.—The goals and priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include—

''(1) encouraging and supporting mechanisms for interdisciplinary research and development in networking and information technology, including—

''(A) through collaborations across agencies;

''(B) through collaborations across Program Component Areas;

''(C) through collaborations with industry;

''(D) through collaborations with institutions of higher education;

''(E) through collaborations with Federal laboratories (as defined in section 4 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3703)); and

''(F) through collaborations with international organizations;

''(2) addressing national, multi-agency, multi-faceted challenges of national importance; and

''(3) fostering the transfer of research and development results into new technologies and applications for the benefit of society.''.

(b) DEVELOPMENT OF STRATEGIC PLAN.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(e) STRATEGIC PLAN.—

''(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the agencies under subsection (a)(3)(B), working through the National Science and Technology Council and with the assistance of the Office of Science and Technology Policy shall develop a 5-year strategic plan to guide the activities under subsection (a)(1).

''(2) CONTENTS.—The strategic plan shall specify—

''(A) the near-term objectives for the Program;

''(B) the long-term objectives for the Program;

''(C) the anticipated time frame for achieving the near-term objectives;

''(D) the metrics that will be used to assess any progress made toward achieving the near-term objectives and the long-term objectives; and

''(E) how the Program will achieve the goals and priorities under subsection (d).

''(3) IMPLEMENTATION ROADMAP.—

''(A) IN GENERAL.—The agencies under subsection (a)(3)(B) shall develop and annually update an implementation roadmap for the strategic plan.

''(B) REQUIREMENTS.—The information in the implementation roadmap shall be coordinated with the database under section 102(c) and the annual report under section 101(a)(3). The implementation roadmap shall—

''(i) specify the role of each Federal agency in carrying out or sponsoring research and development to meet the research objectives of the strategic plan, including a description of how progress toward the research objectives will be evaluated, with consideration of any relevant recommendations of the advisory committee;

''(ii) specify the funding allocated to each major research objective of the strategic plan and the source of funding by agency for the current fiscal year; and

''(iii) estimate the funding required for each major research objective of the strategic plan for the next 3 fiscal years.

''(4) RECOMMENDATIONS.—The agencies under subsection (a)(3)(B) shall take into consideration when developing the strategic plan under paragraph (1) the recommendations of—

''(A) the advisory committee under subsection (b); and

''(B) the stakeholders under section 102(a)(3).

''(5) REPORT TO CONGRESS.—The Director of the Office of Science and Technology Policy shall transmit the strategic plan under this

subsection, including the implementation roadmap and any updates under paragraph (3), to—

''(A) the advisory committee under subsection (b);

''(B) the Committee on Commerce, Science, and Transportation of the Senate; and

''(C) the Committee on Science and Technology of the House of Representatives.''.

(c) PERIODIC REVIEWS.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(f) PERIODIC REVIEWS.—The agencies under subsection (a)(3)(B) shall—

''(1) periodically assess the contents and funding levels of the Program Component Areas and restructure the Program when warranted, taking into consideration any relevant recommendations of the advisory committee under subsection (b); and

''(2) ensure that the Program includes national, multi-agency, multi-faceted research and development activities, including activities described in section 104.''.

(d) ADDITIONAL RESPONSIBILITIES OF DIRECTOR.—Section 101(a)(2) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(2)) is amended—

(1) by redesignating subparagraphs (E) and (F) as subparagraphs (G) and (H), respectively; and

(2) by inserting after subparagraph (D) the following:

''(E) encourage and monitor the efforts of the agencies participating in the Program to allocate the level of resources and management attention necessary—

''(i) to ensure that the strategic plan under subsection (e) is developed and executed effectively; and

''(ii) to ensure that the objectives of the Program are met;

''(F) working with the Office of Management and Budget and in coordination with the creation of the database under section 102(c), direct the Office of Science and Technology Policy and the agencies participating in the Program to establish a mechanism (consistent with existing law) to track all ongoing and completed research and development projects and associated funding;''.

(e) ADVISORY COMMITTEE.—Section 101(b) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(b)) is amended—

(1) in paragraph (1)—

(A) by inserting after the first sentence the following: ''The co-chairs of the advisory committee shall meet the qualifications of committee members and may be members of the Presidents Council of Advisors on Science and Technology.''; and

(B) by striking ''high-performance'' in subparagraph (D) and inserting ''high-end''; and

(2) by amending paragraph (2) to read as follows:

''(2) In addition to the duties under paragraph (1), the advisory committee shall conduct periodic evaluations of the funding, management, coordination, implementation, and activities of the Program. The advisory committee shall report its findings and recommendations not less frequently than once every 3 fiscal years to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives. The report shall be submitted in conjunction with the update of the strategic plan.''.

(f) REPORT.—Section 101(a)(3) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(3)) is amended—

(1) in subparagraph (C)—

(A) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(B) by striking ''each Program Component Area'' and inserting ''each Program Component Area and each research area supported in accordance with section 104'';

(2) in subparagraph (D)—

(A) by striking ''each Program Component Area,'' and inserting ''each Program Component Area and each research area supported in accordance with section 104,'';

(B) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(C) by striking ''and'' after the semicolon;

(3) by redesignating subparagraph (E) as subparagraph (G); and

(4) by inserting after subparagraph (D) the following:

''(E) include a description of how the objectives for each Program Component Area, and the objectives for activities that involve multiple Program Component Areas, relate to the objectives of the Program identified in the strategic plan under subsection (e);

''(F) include—

''(i) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the next fiscal year by category of activity;

''(ii) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the current fiscal year by category of activity; and

''(iii) the amount of funding provided for the Office of Science and Technology Policy for the current fiscal year by each agency participating in the Program; and''.

(g) DEFINITIONS.—Section 4 of the High-Performance Computing Act of 1991 (15 U.S.C. 5503) is amended—

(1) by redesignating paragraphs (1) and (2) as paragraphs (2) and (3), respectively;

(2) by redesignating paragraph (3) as paragraph (6);

(3) by redesignating paragraphs (6) and (7) as paragraphs (7) and (8), respectively;

(4) by inserting before paragraph (2), as redesignated, the following:

''(1) 'cyber-physical systems' means physical or engineered systems whose networking and information technology functions and physical elements are deeply integrated and are actively connected to the physical world through sensors, actuators, or other means to perform monitoring and control functions;'';

(5) in paragraph (3), as redesignated, by striking ''high-performance computing'' and inserting ''networking and information technology'';

(6) in paragraph (6), as redesignated—

(A) by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(B) by striking ''supercomputer'' and inserting ''high-end computing'';

(7) in paragraph (5), by striking ''network referred to as'' and all that follows through the semicolon and inserting ''network, including advanced computer networks of Federal agencies and departments''; and

(8) in paragraph (7), as redesignated, by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program''.

SEC. 402. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

(a) RESEARCH IN AREAS OF NATIONAL IMPORTANCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.) is amended by adding at the end the following:

''SEC. 104. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

''(a) IN GENERAL.—The Program shall encourage agencies under section 101(a)(3)(B) to support, maintain, and improve national, multi-agency, multi-faceted, research and development activities in networking and information technology directed toward application areas that have the potential for significant contributions to national economic competitiveness and for other significant societal benefits.

''(b) TECHNICAL SOLUTIONS.—An activity under subsection (a) shall be designed to advance the development of research discoveries by demonstrating technical solutions to important problems in areas including—

''(1) cybersecurity;

''(2) health care;

''(3) energy management and low-power systems and devices;

''(4) transportation, including surface and air transportation;

''(5) cyber-physical systems;

''(6) large-scale data analysis and modeling of physical phenomena;

''(7) large scale data analysis and modeling of behavioral phenomena;

''(8) supply chain quality and security; and

''(9) privacy protection and protected disclosure of confidential data.

''(c) RECOMMENDATIONS.—The advisory committee under section 101(b) shall make recommendations to the Program for candidate research and development areas for support under this section.

''(d) CHARACTERISTICS.—

''(1) IN GENERAL.—Research and development activities under this section—

''(A) shall include projects selected on the basis of applications for support through a competitive, merit-based process;

''(B) shall leverage, when possible, Federal investments through collaboration with related State initiatives;

''(C) shall include a plan for fostering the transfer of research discoveries and the results of technology demonstration activities, including from institutions of higher education and Federal laboratories, to industry for commercial development;

''(D) shall involve collaborations among researchers in institutions of higher education and industry; and

''(E) may involve collaborations among nonprofit research institutions and Federal laboratories, as appropriate.

''(2) COST-SHARING.—In selecting applications for support, the agencies under section 101(a)(3)(B) shall give special consideration to projects that include cost sharing from non-Federal sources.

''(3) MULTIDISCIPLINARY RESEARCH CENTERS.—Research and development activities under this section shall be supported through multidisciplinary research centers, including Federal laboratories, that are organized to investigate basic research questions and carry out technology demonstration activities in areas described in subsection (a). Research may be carried out through existing multidisciplinary centers, including those authorized under section 7024(b)(2) of the America COMPETES Act (42 U.S.C. 1862o–10(2)).''.

(b) CYBER-PHYSICAL SYSTEMS.—Section 101(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following:

''(J) provide for increased understanding of the scientific principles of cyber-physical systems and improve the methods available for the design, development, and operation of cyber-physical systems that are characterized by high reliability, safety, and security; and

''(K) provide for research and development on human-computer interactions, visualization, and big data.''.

(c) TASK FORCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.), as amended by section 402(a) of this Act, is amended by adding at the end the following:

''SEC. 105. TASK FORCE.

''(a) ESTABLISHMENT.—Not later than 180 days after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy under section 102 shall convene a task force to explore mechanisms for carrying out collaborative research and development activities for cyber-physical systems (including the related technologies required to enable these systems) through a consortium or other appropriate entity with participants from institutions of higher education, Federal laboratories, and industry.

''(b) FUNCTIONS.—The task force shall—

''(1) develop options for a collaborative model and an organizational structure for such entity under which the joint research and development activities could be planned, managed, and conducted effectively, including mechanisms for the allocation of resources among the participants in such entity for support of such activities;

''(2) propose a process for developing a research and development agenda for such entity, including guidelines to ensure an appropriate scope of work focused on nationally significant challenges and requiring collaboration and to ensure the development of related scientific and technological milestones;

''(3) define the roles and responsibilities for the participants from institutions of higher education, Federal laboratories, and industry in such entity;

''(4) propose guidelines for assigning intellectual property rights and for transferring research results to the private sector; and

''(5) make recommendations for how such entity could be funded from Federal, State, and non-governmental sources.

''(c) COMPOSITION.—In establishing the task force under subsection (a), the Director of the Office of Science and Technology Policy shall appoint an equal number of individuals from institutions of higher education and from industry with knowledge and expertise in cyber-physical systems, and may appoint not more than 2 individuals from Federal laboratories.

''(d) REPORT.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy shall transmit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives a report describing the findings and recommendations of the task force.

''(e) TERMINATION.—The task force shall terminate upon transmittal of the report required under subsection (d).

''(f) COMPENSATION AND EXPENSES.—Members of the task force shall serve without compensation.''.

SEC. 403. PROGRAM IMPROVEMENTS.

Section 102 of the High-Performance Computing Act of 1991 (15 U.S.C. 5512) is amended to read as follows:

''SEC. 102. PROGRAM IMPROVEMENTS.

''(a) FUNCTIONS.—The Director of the Office of Science and Technology Policy shall continue—

''(1) to provide technical and administrative support to—

''(A) the agencies participating in planning and implementing the Program, including support needed to develop the strategic plan under section 101(e); and

''(B) the advisory committee under section 101(b);

''(2) to serve as the primary point of contact on Federal networking and information technology activities for government agencies, academia, industry, professional societies, State computing and networking technology programs, interested citizen groups, and others to exchange technical and programmatic information;

''(3) to solicit input and recommendations from a wide range of stakeholders during the development of each strategic plan under section 101(e) by convening at least 1 workshop with invitees from academia, industry, Federal laboratories, and other relevant organizations and institutions;

''(4) to conduct public outreach, including the dissemination of the advisory committee's findings and recommendations, as appropriate;

''(5) to promote access to and early application of the technologies, innovations, and expertise derived from Program activities to agency missions and systems across the Federal Government and to United States industry;

''(6) to ensure accurate and detailed budget reporting of networking and information technology research and development investment; and

''(7) to encourage agencies participating in the Program to use existing programs and resources to strengthen networking and information technology education and training, and increase participation in such fields, including by women and underrepresented minorities.

''(b) SOURCE OF FUNDING.—

''(1) IN GENERAL.—The functions under this section shall be supported by funds from each agency participating in the Program.

''(2) SPECIFICATIONS.—The portion of the total budget of the Office of Science and Technology Policy that is provided by each agency participating in the Program for each fiscal year shall be in the same proportion as each agency's share of the total budget for the Program for the previous fiscal year, as specified in the database under section 102(c).

''(c) DATABASE.—

''(1) IN GENERAL.—The Director of the Office of Science and Technology Policy shall develop and maintain a database of projects funded by each agency for the fiscal year for each Program Component Area.

''(2) PUBLIC ACCESSIBILITY.—The Director of the Office of Science and Technology Policy shall make the database accessible to the public.

''(3) DATABASE CONTENTS.—The database shall include, for each project in the database—

''(A) a description of the project;

''(B) each agency, industry, institution of higher education, Federal laboratory, or international institution involved in the project;

''(C) the source funding of the project (set forth by agency);

''(D) the funding history of the project; and

''(E) whether the project has been completed.''.

SEC. 404. IMPROVING EDUCATION OF NETWORKING AND INFORMATION TECHNOLOGY, INCLUDING HIGH PERFORMANCE COMPUTING.

Section 201(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)) is amended—

(1) by redesignating paragraphs (2) through (4) as paragraphs (3) through (5), respectively; and

(2) by inserting after paragraph (1) the following:

''(2) the National Science Foundation shall use its existing programs, in collaboration with other agencies, as appropriate, to improve the teaching and learning of networking and information technology at all levels of education and to increase participation in networking and information technology fields;''.

SEC. 405. CONFORMING AND TECHNICAL AMENDMENTS TO THE HIGH-PERFORMANCE COMPUTING ACT OF 1991.

(a) SECTION 3.—Section 3 of the High-Performance Computing Act of 1991 (15 U.S.C. 5502) is amended—

(1) in the matter preceding paragraph (1), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(2) in paragraph (1)—

(A) in the matter preceding subparagraph (A), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(B) in subparagraphs (A), (F), and (G), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(C) in subparagraph (H), by striking ''high-performance'' and inserting ''high-end''; and

(3) in paragraph (2)—

(A) by striking ''high-performance computing and'' and inserting ''networking and information technology, and''; and

(B) by striking ''high-performance computing network'' and inserting ''networking and information technology''.

(b) TITLE HEADING.—The heading of title I of the High-Performance Computing Act of 1991 (105 Stat. 1595) is amended by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''.

(c) SECTION 101.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT**'';

(2) in subsection (a)—

(A) in the subsection heading, by striking ''NATIONAL HIGH-PERFORMANCE COMPUTING'' and inserting ''NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT'';

(B) in paragraph (1)—

(i) by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program'';

(ii) in subparagraph (A), by striking ''high-performance computing, including networking'' and inserting ''networking and information technology'';

(iii) in subparagraphs (B) and (G), by striking ''high-performance'' each place it appears and inserting ''high-end''; and

(iv) in subparagraph (C), by striking ''high-performance computing and networking'' and inserting ''high-end computing, distributed, and networking''; and

(C) in paragraph (2)—

(i) in subparagraphs (A) and (C)—

(I) by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(II) by striking ''development, networking,'' each place it appears and inserting ''development,''; and

(ii) in subparagraphs (G) and (H), as redesignated by section 401(d) of this Act, by striking ''high-performance'' each place it appears and inserting ''high-end'';

(3) in subsection (b)(1), in the matter preceding subparagraph (A), by striking ''high-

performance computing'' each place it appears and inserting ''networking and information technology''; and

(4) in subsection (c)(1)(A), by striking ''high-performance computing'' and inserting ''networking and information technology''.

(d) SECTION 201.—Section 201(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)(1)) is amended by striking ''high-performance computing and advanced high-speed computer networking'' and inserting ''networking and information technology research and development''.

(e) SECTION 202.—Section 202(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5522(a)) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(f) SECTION 203.—Section 203(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5523(a)) is amended—

(1) in paragraph (1), by striking ''high-performance computing and networking'' and inserting ''networking and information technology''; and

(2) in paragraph (2)(A), by striking ''high-performance'' and inserting ''high-end''.

(g) SECTION 204.—Section 204 of the High-Performance Computing Act of 1991 (15 U.S.C. 5524) is amended—

(1) in subsection (a)(1)—

(A) in subparagraph (A), by striking ''high-performance computing systems and networks'' and inserting ''networking and information technology systems and capabilities'';

(B) in subparagraph (B), by striking ''interoperability of high-performance computing systems in networks and for common user interfaces to systems'' and inserting ''interoperability and usability of networking and information technology systems''; and

(C) in subparagraph (C), by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(2) in subsection (b)—

(A) by striking ''HIGH-PERFORMANCE COMPUTING AND NETWORK'' in the heading and inserting ''NETWORKING AND INFORMATION TECHNOLOGY''; and

(B) by striking ''sensitive''.

(h) SECTION 205.—Section 205(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5525(a)) is amended by striking ''computational'' and inserting ''networking and information technology''.

(i) SECTION 206.—Section 206(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5526(a)) is amended by striking ''computational research'' and inserting ''networking and information technology research''.

(j) SECTION 207.—Section 207 of the High-Performance Computing Act of 1991 (15 U.S.C. 5527) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(k) SECTION 208.—Section 208 of the High-Performance Computing Act of 1991 (15 U.S.C. 5528) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''; and

(2) in subsection (a)—

(A) in paragraph (1), by striking ''High-performance computing and associated'' and inserting ''Networking and information'';

(B) in paragraph (2), by striking ''high-performance computing'' and inserting ''networking and information technologies'';

(C) in paragraph (3), by striking ''high-performance'' and inserting ''high-end'';

(D) in paragraph (4), by striking ''high-performance computers and associated'' and inserting ''networking and information''; and

(E) in paragraph (5), by striking ''high-performance computing and associated'' and inserting ''networking and information''.

SEC. 406. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation, in coordination with the Secretary of Homeland Security, shall carry out a Federal cyber scholarship-for-service program to recruit and train the next generation of information technology professionals and security managers to meet the needs of the cybersecurity mission for the Federal government.

(b) PROGRAM DESCRIPTION AND COMPONENTS.—The program shall—

(1) annually assess the workforce needs of the Federal government for cybersecurity professionals, including network engineers, software engineers, and other experts in order to determine how many scholarships should be awarded annually to ensure that the workforce needs following graduation match the number of scholarships awarded;

(2) provide scholarships for up to 1,000 students per year in their pursuit of undergraduate or graduate degrees in the cybersecurity field, in an amount that may include coverage for full tuition, fees, and a stipend;

(3) require each scholarship recipient, as a condition of receiving a scholarship under the program, to serve in a Federal information technology workforce for a period equal to one and one-half times each year, or partial year, of scholarship received, in addition to an internship in the cybersecurity field, if applicable, following graduation;

(4) provide a procedure for the National Science Foundation or a Federal agency, consistent with regulations of the Office of Personnel Management, to request and fund a security clearance for a scholarship recipient, including providing for clearance during a summer internship and upon graduation; and

(5) provide opportunities for students to receive temporary appointments for meaningful employment in the Federal information technology workforce during school vacation periods and for internships.

(c) HIRING AUTHORITY.—

(1) IN GENERAL.—For purposes of any law or regulation governing the appointment of an individual in the Federal civil service, upon the successful completion of the student's studies, a student receiving a scholarship under the program may—

(A) be hired under section 213.3102(r) of title 5, Code of Federal Regulations; and

(B) be exempt from competitive service.

(2) COMPETITIVE SERVICE.—Upon satisfactory fulfillment of the service term under paragraph (1), an individual may be converted to a competitive service position without competition if the individual meets the requirements for that position.

(d) ELIGIBILITY.—The eligibility requirements for a scholarship under this section shall include that a scholarship applicant—

(1) be a citizen of the United States;

(2) be eligible to be granted a security clearance;

(3) maintain a grade point average of 3.2 or above on a 4.0 scale for undergraduate study or a 3.5 or above on a 4.0 scale for post-graduate study;

(4) demonstrate a commitment to a career in improving the security of the information infrastructure; and

(5) has demonstrated a level of proficiency in math or computer sciences.

(e) FAILURE TO COMPLETE SERVICE OBLIGATION.—

(1) IN GENERAL.—A scholarship recipient under this section shall be liable to the United States under paragraph (2) if the scholarship recipient—

(A) fails to maintain an acceptable level of academic standing in the educational institution in which the individual is enrolled, as determined by the Director;

(B) is dismissed from such educational institution for disciplinary reasons;

(C) withdraws from the program for which the award was made before the completion of such program;

(D) declares that the individual does not intend to fulfill the service obligation under this section;

(E) fails to fulfill the service obligation of the individual under this section; or

(F) loses a security clearance or becomes ineligible for a security clearance.

(2) REPAYMENT AMOUNTS.—

(A) LESS THAN 1 YEAR OF SERVICE.—If a circumstance under paragraph (1) occurs before the completion of 1 year of a service obligation under this section, the total amount of awards received by the individual under this section shall be repaid.

(B) ONE OR MORE YEARS OF SERVICE.—If a circumstance described in subparagraph (D) or (E) of paragraph (1) occurs after the completion of 1 year of a service obligation under this section, the total amount of scholarship awards received by the individual under this section, reduced by the ratio of the number of years of service completed divided by the number of years of service required, shall be repaid.

(f) EVALUATION AND REPORT.—The Director of the National Science Foundation shall—

(1) evaluate the success of recruiting individuals for scholarships under this section and of hiring and retaining those individuals in the public sector workforce, including the annual cost and an assessment of how the program actually improves the Federal workforce; and

(2) periodically report the findings under paragraph (1) to Congress.

(g) AUTHORIZATION OF APPROPRIATIONS.—From amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), the Director may use funds to carry out the requirements of this section for fiscal years 2012 through 2013.

SEC. 407. STUDY AND ANALYSIS OF CERTIFICATION AND TRAINING OF INFORMATION INFRASTRUCTURE PROFESSIONALS.

(a) STUDY.—The President shall enter into an agreement with the National Academies to conduct a comprehensive study of government, academic, and private-sector accreditation, training, and certification programs for personnel working in information infrastructure. The agreement shall require the National Academies to consult with sector coordinating councils and relevant governmental agencies, regulatory entities, and nongovernmental organizations in the course of the study.

(b) SCOPE.—The study shall include—

(1) an evaluation of the body of knowledge and various skills that specific categories of personnel working in information infrastructure should possess in order to secure information systems;

(2) an assessment of whether existing government, academic, and private-sector accreditation, training, and certification programs provide the body of knowledge and various skills described in paragraph (1);

(3) an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity talent, including barriers relating to compensation, the hiring process, job classification, and hiring flexibility; and

(4) an analysis of the sources and availability of cybersecurity talent, a comparison of the skills and expertise sought by the Federal Government and the private sector, an examination of the current and future capacity of United States institutions of higher

education, including community colleges, to provide current and future cybersecurity professionals, through education and training activities, with those skills sought by the Federal Government, State and local entities, and the private sector.

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the National Academies shall submit to the President and Congress a report on the results of the study. The report shall include—

(1) findings regarding the state of information infrastructure accreditation, training, and certification programs, including specific areas of deficiency and demonstrable progress; and

(2) recommendations for the improvement of information infrastructure accreditation, training, and certification programs.

SEC. 408. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

(a) IN GENERAL.—The Director of the National Institute of Standards and Technology, in coordination with appropriate Federal authorities, shall—

(1) as appropriate, ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to Congress a plan for ensuring such Federal agency coordination.

(b) CONSULTATION WITH THE PRIVATE SECTOR.—In carrying out the activities under subsection (a)(1), the Director shall ensure consultation with appropriate private sector stakeholders.

SEC. 409. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

The Director of the National Institute of Standards and Technology shall continue a program to support the development of technical standards, metrology, testbeds, and conformance criteria, taking into account appropriate user concerns—

(1) to improve interoperability among identity management technologies;

(2) to strengthen authentication methods of identity management systems;

(3) to improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols; and

(4) to improve the usability of identity management systems.

SEC. 410. FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY RESEARCH GRANT AREAS.—Section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking ''property.'' and inserting ''property;''; and

(3) by adding at the end the following:

''(J) secure fundamental protocols that are at the heart of inter-network communications and data exchange;

''(K) system security that addresses the building of secure systems from trusted and untrusted components;

''(L) monitoring and detection; and

''(M) resiliency and rapid recovery methods.''.

(b) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY GRANTS.—Section 4(a)(3) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(3)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(c) COMPUTER AND NETWORK SECURITY CENTERS.—Section 4(b)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7403(b)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(d) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—Section 5(a)(6) of the Cyber Security Research and Development Act (15 U.S.C. 7404(a)(6)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT GRANTS.—Section 5(b)(2) of the Cyber Security Research and Development Act (15 U.S.C. 7404(b)(2)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(f) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY RESEARCH.—Section 5(c)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7404(c)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

SA 2615. Mrs. HUTCHISON submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 45, strike line 1 and all that follows through page 212, line 6, and insert the following:

TITLE II—FACILITATING SHARING OF CYBER THREAT INFORMATION

SEC. 201. DEFINITIONS.

In this title:

(1) AGENCY.—The term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code.

(2) ANTITRUST LAWS.—The term ''antitrust laws''—

(A) has the meaning given the term in section 1(a) of the Clayton Act (15 U.S.C. 12(a));

(B) includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that section 5 of that Act applies to unfair methods of competition; and

(C) includes any State law that has the same intent and effect as the laws under subparagraphs (A) and (B).

(3) COUNTERMEASURE.—The term ''countermeasure'' means an automated or a manual action with defensive intent to mitigate cyber threats.

(4) CYBER THREAT INFORMATION.—The term ''cyber threat information'' means information that indicates or describes—

(A) a technical or operation vulnerability or a cyber threat mitigation measure;

(B) an action or operation to mitigate a cyber threat;

(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

(D) a method of defeating a technical control;

(E) a method of defeating an operational control;

(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

(G) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to inadvertently enable the defeat of a technical or operational control;

(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

(J) any combination of subparagraphs (A) through (I).

(5) CYBERSECURITY CENTER.—The term ''cybersecurity center'' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

(6) CYBERSECURITY SYSTEM.—The term ''cybersecurity system'' means a system designed or employed to ensure the integrity, confidentiality, or availability of, or to safeguard, a system or network, including measures intended to protect a system or network from—

(A) efforts to degrade, disrupt, or destroy such system or network; or

(B) theft or misappropriations of private or government information, intellectual property, or personally identifiable information.

(7) ENTITY.—

(A) IN GENERAL.—The term ''entity'' means any private entity, non-Federal government agency or department, or State, tribal, or local government agency or department (including an officer, employee, or agent thereof).

(B) INCLUSIONS.—The term ''entity'' includes a government agency or department (including an officer, employee, or agent thereof) of the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States.

(8) FEDERAL INFORMATION SYSTEM.—The term ''Federal information system'' means an information system of a Federal department or agency used or operated by an executive agency, by a contractor of an executive

agency, or by another organization on behalf of an executive agency.

(9) INFORMATION SECURITY.—The term ''information security'' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; or

(C) availability, by ensuring timely and reliable access to and use of information.

(10) INFORMATION SYSTEM.—The term ''information system'' has the meaning given the term in section 3502 of title 44, United States Code.

(11) LOCAL GOVERNMENT.—The term ''local government'' means any borough, city, county, parish, town, township, village, or other general purpose political subdivision of a State.

(12) MALICIOUS RECONNAISSANCE.—The term ''malicious reconnaissance'' means a method for actively probing or passively monitoring an information system for the purpose of discerning technical vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(13) OPERATIONAL CONTROL.—The term ''operational control'' means a security control for an information system that primarily is implemented and executed by people.

(14) OPERATIONAL VULNERABILITY.—The term ''operational vulnerability'' means any attribute of policy, process, or procedure that could enable or facilitate the defeat of an operational control.

(15) PRIVATE ENTITY.—The term ''private entity'' means any individual or any private group, organization, or corporation, including an officer, employee, or agent thereof.

(16) SIGNIFICANT CYBER INCIDENT.—The term ''significant cyber incident'' means a cyber incident resulting in, or an attempted cyber incident that, if successful, would have resulted in—

(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

(17) TECHNICAL CONTROL.—The term ''technical control'' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

(18) TECHNICAL VULNERABILITY.—The term ''technical vulnerability'' means any attribute of hardware or software that could enable or facilitate the defeat of a technical control.

(19) TRIBAL.—The term ''tribal'' has the meaning given the term ''Indian tribe'' in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

SEC. 202. AUTHORIZATION TO SHARE CYBER THREAT INFORMATION.

(a) VOLUNTARY DISCLOSURE.—

(1) PRIVATE ENTITIES.—Notwithstanding any other provision of law, a private entity may, for the purpose of preventing, investigating, or otherwise mitigating threats to information security, on its own networks, or as authorized by another entity, on such entity's networks, employ countermeasures and use cybersecurity systems in order to obtain, identify, or otherwise possess cyber threat information.

(2) ENTITIES.—Notwithstanding any other provision of law, an entity may disclose cyber threat information to—

(A) a cybersecurity center; or

(B) any other entity in order to assist with preventing, investigating, or otherwise mitigating threats to information security.

(3) INFORMATION SECURITY PROVIDERS.—If the cyber threat information described in paragraph (1) is obtained, identified, or otherwise possessed in the course of providing information security products or services under contract to another entity, that entity shall be given, at any time prior to disclosure of such information, a reasonable opportunity to authorize or prevent such disclosure, to request anonymization of such information, or to request that reasonable efforts be made to safeguard such information that identifies specific persons from unauthorized access or disclosure.

(b) SIGNIFICANT CYBER INCIDENTS INVOLVING FEDERAL INFORMATION SYSTEMS.—

(1) IN GENERAL.—An entity providing electronic communication services, remote computing services, or information security services to a Federal department or agency shall inform the Federal department or agency of a significant cyber incident involving the Federal information system of that Federal department or agency that—

(A) is directly known to the entity as a result of providing such services;

(B) is directly related to the provision of such services by the entity; and

(C) as determined by the entity, has impeded or will impede the performance of a critical mission of the Federal department or agency.

(2) ADVANCE COORDINATION.—A Federal department or agency receiving the services described in paragraph (1) shall coordinate in advance with an entity described in paragraph (1) to develop the parameters of any information that may be provided under paragraph (1), including clarification of the type of significant cyber incident that will impede the performance of a critical mission of the Federal department or agency.

(3) REPORT.—A Federal department or agency shall report information provided under this subsection to a cybersecurity center.

(4) CONSTRUCTION.—Any information provided to a cybersecurity center under paragraph (3) shall be treated in the same manner as information provided to a cybersecurity center under subsection (a).

(c) INFORMATION SHARED WITH OR PROVIDED TO A CYBERSECURITY CENTER.—Cyber threat information provided to a cybersecurity center under this section—

(1) may be disclosed to, retained by, and used by, consistent with otherwise applicable Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal government for a cybersecurity purpose, a national security purpose, or in order to prevent, investigate, or prosecute any of the offenses listed in section 2516 of title 18, United States Code, and such information shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under this paragraph;

(2) may, with the prior written consent of the entity submitting such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(3) shall be considered the commercial, financial, or proprietary information of the entity providing such information to the Federal government and any disclosure outside the Federal government may only be made upon the prior written consent by such entity and shall not constitute a waiver of any applicable privilege or protection provided by law, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(4) shall be deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records;

(5) shall be, without discretion, withheld from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records;

(6) shall not be subject to the rules of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official;

(7) shall not, if subsequently provided to a State, tribal, or local government or government agency, otherwise be disclosed or distributed to any entity by such State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent; and

(8) shall not be directly used by any Federal, State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph.

(d) PROCEDURES RELATING TO INFORMATION SHARING WITH A CYBERSECURITY CENTER.—Not later than 60 days after the date of enactment of this Act, the heads of each department or agency containing a cybersecurity center shall jointly develop, promulgate, and submit to Congress procedures to ensure that cyber threat information shared with or provided to—

(1) a cybersecurity center under this section—

(A) may be submitted to a cybersecurity center by an entity, to the greatest extent possible, through a uniform, publicly available process or format that is easily accessible on the website of such cybersecurity center, and that includes the ability to provide relevant details about the cyber threat information and written consent to any subsequent disclosures authorized by this paragraph;

(B) shall immediately be further shared with each cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government;

(C) is handled by the Federal government in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title, and the Federal government may undertake efforts consistent with this

subparagraph to limit the impact on privacy and civil liberties of the sharing of cyber threat information with the Federal government; and

(D) except as provided in this section, shall only be used, disclosed, or handled in accordance with the provisions of subsection (c); and

(2) a Federal agency or department under subsection (b) is provided immediately to a cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government.

(e) INFORMATION SHARED BETWEEN ENTITIES.—

(1) IN GENERAL.—An entity sharing cyber threat information with another entity under this title may restrict the use or sharing of such information by such other entity.

(2) FURTHER SHARING.—Cyber threat information shared by any entity with another entity under this title—

(A) shall only be further shared in accordance with any restrictions placed on the sharing of such information by the entity authorizing such sharing, such as appropriate anonymization of such information; and

(B) may not be used by any entity to gain an unfair competitive advantage to the detriment of the entity authorizing the sharing of such information, except that the conduct described in paragraph (3) shall not constitute unfair competitive conduct.

(3) INFORMATION SHARED WITH STATE, TRIBAL, OR LOCAL GOVERNMENT OR GOVERNMENT AGENCY.—Cyber threat information shared with a State, tribal, or local government or government agency under this title—

(A) may, with the prior written consent of the entity sharing such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent;

(B) shall be deemed voluntarily shared information and exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records;

(C) shall not be disclosed or distributed to any entity by the State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent; and

(D) shall not be directly used by any State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this subparagraph.

(4) ANTITRUST EXEMPTION.—The exchange or provision of cyber threat information or assistance between 2 or more private entities under this title shall not be considered a violation of any provision of antitrust laws if exchanged or provided in order to assist with—

(A) facilitating the prevention, investigation, or mitigation of threats to information security; or

(B) communicating or disclosing of cyber threat information to help prevent, investigate or otherwise mitigate the effects of a threat to information security.

(5) NO RIGHT OR BENEFIT.—The provision of cyber threat information to an entity under this section shall not create a right or a benefit to similar information by such entity or any other entity.

(f) FEDERAL PREEMPTION.—

(1) IN GENERAL.—This section supersedes any statute or other law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this section.

(2) STATE LAW ENFORCEMENT.—Nothing in this section shall be construed to supersede any statute or other law of a State or political subdivision of a State concerning the use of authorized law enforcement techniques.

(3) PUBLIC DISCLOSURE.—No information shared with or provided to a State, tribal, or local government or government agency pursuant to this section shall be made publicly available pursuant to any State, tribal, or local law requiring disclosure of information or records.

(g) CIVIL AND CRIMINAL LIABILITY.—

(1) GENERAL PROTECTIONS.—

(A) PRIVATE ENTITIES.—No cause of action shall lie or be maintained in any court against any private entity for—

(i) the use of countermeasures and cybersecurity systems as authorized by this title;

(ii) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(iii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such private entity.

(B) ENTITIES.—No cause of action shall lie or be maintained in any court against any entity for—

(i) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(ii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such entity.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed as creating any immunity against, or otherwise affecting, any action brought by the Federal government, or any agency or department thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, and use of classified information.

(h) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this section shall be construed to limit or prohibit otherwise lawful disclosures of communications, records, or other information by a private entity to any other governmental or private entity not covered under this section.

(i) WHISTLEBLOWER PROTECTION.—Nothing in this Act shall be construed to preempt or preclude any employee from exercising rights currently provided under any whistleblower law, rule, or regulation.

(j) RELATIONSHIP TO OTHER LAWS.—The submission of cyber threat information under this section to a cybersecurity center shall not affect any requirement under any other provision of law for an entity to provide information to the Federal government.

SEC. 203. INFORMATION SHARING BY THE FEDERAL GOVERNMENT.

(a) CLASSIFIED INFORMATION.—

(1) PROCEDURES.—Consistent with the protection of intelligence sources and methods, and as otherwise determined appropriate, the Director of National Intelligence and the Secretary of Defense, in consultation with the heads of the appropriate Federal departments or agencies, shall develop and promulgate procedures to facilitate and promote—

(A) the immediate sharing, through the cybersecurity centers, of classified cyber threat information in the possession of the Federal government with appropriately cleared representatives of any appropriate entity; and

(B) the declassification and immediate sharing, through the cybersecurity centers, with any entity or, if appropriate, public availability of cyber threat information in the possession of the Federal government;

(2) HANDLING OF CLASSIFIED INFORMATION.—The procedures developed under paragraph (1) shall ensure that each entity receiving classified cyber threat information pursuant to this section has acknowledged in writing the ongoing obligation to comply with all laws, executive orders, and procedures concerning the appropriate handling, disclosure, or use of classified information.

(b) UNCLASSIFIED CYBER THREAT INFORMATION.—The heads of each department or agency containing a cybersecurity center shall jointly develop and promulgate procedures that ensure that, consistent with the provisions of this section, unclassified, including controlled unclassified, cyber threat information in the possession of the Federal government—

(1) is shared, through the cybersecurity centers, in an immediate and adequate manner with appropriate entities; and

(2) if appropriate, is made publicly available.

(c) DEVELOPMENT OF PROCEDURES.—

(1) IN GENERAL.—The procedures developed under this section shall incorporate, to the greatest extent possible, existing processes utilized by sector specific information sharing and analysis centers.

(2) COORDINATION WITH ENTITIES.—In developing the procedures required under this section, the Director of National Intelligence and the heads of each department or agency containing a cybersecurity center shall coordinate with appropriate entities to ensure that protocols are implemented that will facilitate and promote the sharing of cyber threat information by the Federal government.

(d) ADDITIONAL RESPONSIBILITIES OF CYBERSECURITY CENTERS.—Consistent with section 202, a cybersecurity center shall—

(1) facilitate information sharing, interaction, and collaboration among and between cybersecurity centers and—

(A) other Federal entities;

(B) any entity; and

(C) international partners, in consultation with the Secretary of State;

(2) disseminate timely and actionable cybersecurity threat, vulnerability, mitigation, and warning information, including alerts, advisories, indicators, signatures, and mitigation and response measures, to improve the security and protection of information systems; and

(3) coordinate with other Federal entities, as appropriate, to integrate information from across the Federal government to provide situational awareness of the cybersecurity posture of the United States.

(e) SHARING WITHIN THE FEDERAL GOVERNMENT.—The heads of appropriate Federal departments and agencies shall ensure that cyber threat information in the possession of such Federal departments or agencies that relates to the prevention, investigation, or mitigation of threats to information security across the Federal government is shared effectively with the cybersecurity centers.

(f) SUBMISSION TO CONGRESS.—Not later than 60 days after the date of enactment of this Act, the Director of National Intelligence, in coordination with the appropriate head of a department or an agency containing a cybersecurity center, shall submit the procedures required by this section to Congress.

SEC. 204. CONSTRUCTION.

(a) INFORMATION SHARING RELATIONSHIPS.—Nothing in this title shall be construed—

(1) to limit or modify an existing information sharing relationship;

(2) to prohibit a new information sharing relationship;

(3) to require a new information sharing relationship between any entity and the Federal government, except as specified under section 202(b); or

(4) to modify the authority of a department or agency of the Federal government to protect sources and methods and the national security of the United States.

(b) ANTI-TASKING RESTRICTION.—Nothing in this title shall be construed to permit the Federal government—

(1) to require an entity to share information with the Federal government, except as expressly provided under section 202(b); or

(2) to condition the sharing of cyber threat information with an entity on such entity's provision of cyber threat information to the Federal government.

(c) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this title shall be construed to subject any entity to liability for choosing not to engage in the voluntary activities authorized under this title.

(d) USE AND RETENTION OF INFORMATION.—Nothing in this title shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal government to retain or use any information shared under section 202 for any use other than a use permitted under section 202(c)(1).

(e) NO NEW FUNDING.—An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 205. REPORT ON IMPLEMENTATION.

(a) CONTENT OF REPORT.—Not later than 1 year after the date of enactment of this Act, and biennially thereafter, the heads of each department or agency containing a cybersecurity center shall jointly submit, in coordination with the privacy and civil liberties officials of such departments or agencies and the Privacy and Civil Liberties Oversight Board, a detailed report to Congress concerning the implementation of this title, including—

(1) an assessment of the sufficiency of the procedures developed under section 203 of this Act in ensuring that cyber threat information in the possession of the Federal government is provided in an immediate and adequate manner to appropriate entities or, if appropriate, is made publicly available;

(2) an assessment of whether information has been appropriately classified and an accounting of the number of security clearances authorized by the Federal government for purposes of this title;

(3) a review of the type of cyber threat information shared with a cybersecurity center under section 202 of this Act, including whether such information meets the definition of cyber threat information under section 201, the degree to which such information may impact the privacy and civil liberties of individuals, any appropriate metrics to determine any impact of the sharing of such information with the Federal government on privacy and civil liberties, and the adequacy of any steps taken to reduce such impact;

(4) a review of actions taken by the Federal government based on information provided to a cybersecurity center under section 202 of this Act, including the appropriateness of any subsequent use under section 202(c)(1) of this Act and whether there was inappropriate stovepiping within the Federal government of any such information;

(5) a description of any violations of the requirements of this title by the Federal government;

(6) a classified list of entities that received classified information from the Federal government under section 203 of this Act and a description of any indication that such information may not have been appropriately handled;

(7) a summary of any breach of information security, if known, attributable to a specific failure by any entity or the Federal government to act on cyber threat information in the possession of such entity or the Federal government that resulted in substantial economic harm or injury to a specific entity or the Federal government; and

(8) any recommendation for improvements or modifications to the authorities under this title.

(b) FORM OF REPORT.—The report under subsection (a) shall be submitted in unclassified form, but shall include a classified annex.

SEC. 206. INSPECTOR GENERAL REVIEW.

(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency are authorized to review compliance by the cybersecurity centers, and by any Federal department or agency receiving cyber threat information from such cybersecurity centers, with the procedures required under section 202 of this Act.

(b) SCOPE OF REVIEW.—The review under subsection (a) shall consider whether the Federal government has handled such cyber threat information in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title.

(c) REPORT TO CONGRESS.—Each review conducted under this section shall be provided to Congress not later than 30 days after the date of completion of the review.

SEC. 207. TECHNICAL AMENDMENTS.

Section 552(b) of title 5, United States Code, is amended—

(1) in paragraph (8), by striking ''or'';

(2) in paragraph (9), by striking ''wells.'' and inserting ''wells; or''; and

(3) by adding at the end the following:

''(10) information shared with or provided to a cybersecurity center under section 202 of title II of the Cybersecurity Act of 2012.''.

SEC. 208. ACCESS TO CLASSIFIED INFORMATION.

(a) AUTHORIZATION REQUIRED.—No person shall be provided with access to classified information (as defined in section 6.1 of Executive Order 13526 (50 U.S.C. 435 note; relating to classified national security information)) relating to cyber security threats or cyber security vulnerabilities under this title without the appropriate security clearances.

(b) SECURITY CLEARANCES.—The appropriate Federal agencies or departments shall, consistent with applicable procedures and requirements, and if otherwise deemed appropriate, assist an individual in timely obtaining an appropriate security clearance where such individual has been determined to be eligible for such clearance and has a need-to-know (as defined in section 6.1 of that Executive Order) classified information to carry out this title.

TITLE III—COORDINATION OF FEDERAL INFORMATION SECURITY POLICY

SEC. 301. COORDINATION OF FEDERAL INFORMATION SECURITY POLICY.

(a) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by striking subchapters II and III and inserting the following:

''SUBCHAPTER II—INFORMATION SECURITY

''§ 3551. Purposes

''The purposes of this subchapter are—

''(1) to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

''(2) to recognize the highly networked nature of the current Federal computing environment and provide effective government-wide management of policies, directives, standards, and guidelines, as well as effective and nimble oversight of and response to information security risks, including coordination of information security efforts throughout the Federal civilian, national security, and law enforcement communities;

''(3) to provide for development and maintenance of controls required to protect agency information and information systems and contribute to the overall improvement of agency information security posture;

''(4) to provide for the development of tools and methods to assess and respond to real-time situational risk for Federal information system operations and assets; and

''(5) to provide a mechanism for improving agency information security programs through continuous monitoring of agency information systems and streamlined reporting requirements rather than overly prescriptive manual reporting.

''§ 3552. Definitions

''In this subchapter:

''(1) ADEQUATE SECURITY.—The term 'adequate security' means security commensurate with the risk and magnitude of the harm resulting from the unauthorized access to or loss, misuse, destruction, or modification of information.

''(2) AGENCY.—The term 'agency' has the meaning given the term in section 3502 of title 44.

''(3) CYBERSECURITY CENTER.—The term 'cybersecurity center' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

''(4) CYBER THREAT INFORMATION.—The term 'cyber threat information' means information that indicates or describes—

''(A) a technical or operation vulnerability or a cyber threat mitigation measure;

''(B) an action or operation to mitigate a cyber threat;

''(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

''(D) a method of defeating a technical control;

''(E) a method of defeating an operational control;

''(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

''(G) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to inadvertently enable the defeat of a technical or operational control;

''(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

''(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

''(J) any combination of subparagraphs (A) through (I).

''(5) DIRECTOR.—The term 'Director' means the Director of the Office of Management and Budget unless otherwise specified.

''(6) ENVIRONMENT OF OPERATION.—The term 'environment of operation' means the information system and environment in which those systems operate, including changing threats, vulnerabilities, technologies, and missions and business practices.

''(7) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

''(8) INCIDENT.—The term 'incident' means an occurrence that—

''(A) actually or imminently jeopardizes the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores, or transmits; or

''(B) constitutes a violation of law or an imminent threat of violation of a law, a security policy, a security procedure, or an acceptable use policy.

''(9) INFORMATION RESOURCES.—The term 'information resources' has the meaning given the term in section 3502 of title 44.

''(10) INFORMATION SECURITY.—The term 'information security' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

''(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

''(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; or

''(C) availability, by ensuring timely and reliable access to and use of information.

''(11) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44.

''(12) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given the term in section 11101 of title 40.

''(13) MALICIOUS RECONNAISSANCE.—The term 'malicious reconnaissance' means a method for actively probing or passively monitoring an information system for the purpose of discerning technical vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

''(14) NATIONAL SECURITY SYSTEM.—

''(A) IN GENERAL.—The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

''(i) the function, operation, or use of which—

''(I) involves intelligence activities;

''(II) involves cryptologic activities related to national security;

''(III) involves command and control of military forces;

''(IV) involves equipment that is an integral part of a weapon or weapons system; or

''(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

''(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

''(B) LIMITATION.—Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

''(15) OPERATIONAL CONTROL.—The term 'operational control' means a security control for an information system that primarily is implemented and executed by people.

''(16) PERSON.—The term 'person' has the meaning given the term in section 3502 of title 44.

''(17) SECRETARY.—The term 'Secretary' means the Secretary of Commerce unless otherwise specified.

''(18) SECURITY CONTROL.—The term 'security control' means the management, operational, and technical controls, including safeguards or countermeasures, prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

''(19) SIGNIFICANT CYBER INCIDENT.—The term 'significant cyber incident' means a cyber incident resulting in, or an attempted cyber incident that, if successful, would have resulted in—

''(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

''(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

''(20) TECHNICAL CONTROL.—The term 'technical control' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

''§ 3553. Federal information security authority and coordination

''(a) IN GENERAL.—The Secretary, in consultation with the Secretary of Homeland Security, shall—

''(1) issue compulsory and binding policies and directives governing agency information security operations, and require implementation of such policies and directives, including—

''(A) policies and directives consistent with the standards and guidelines promulgated under section 11331 of title 40 to identify and provide information security protections prioritized and commensurate with the risk and impact resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by or on behalf of an agency; or

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(B) minimum operational requirements for Federal Government to protect agency information systems and provide common situational awareness across all agency information systems;

''(C) reporting requirements, consistent with relevant law, regarding information security incidents and cyber threat information;

''(D) requirements for agencywide information security programs;

''(E) performance requirements and metrics for the security of agency information systems;

''(F) training requirements to ensure that agencies are able to fully and timely comply with the policies and directives issued by the Secretary under this subchapter;

''(G) training requirements regarding privacy, civil rights, and civil liberties, and information oversight for agency information security personnel;

''(H) requirements for the annual reports to the Secretary under section 3554(d);

''(I) any other information security operations or information security requirements as determined by the Secretary in coordination with relevant agency heads; and

''(J) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

''(2) review the agencywide information security programs under section 3554; and

''(3) designate an individual or an entity at each cybersecurity center, among other responsibilities—

''(A) to receive reports and information about information security incidents, cyber threat information, and deterioration of security control affecting agency information systems; and

''(B) to act on or share the information under subparagraph (A) in accordance with this subchapter.

''(b) CONSIDERATIONS.—When issuing policies and directives under subsection (a), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology under section 11331 of title 40.

''(c) LIMITATION OF AUTHORITY.—The authorities of the Secretary under this section shall not apply to national security systems. Information security policies, directives, standards and guidelines for national security systems shall be overseen as directed by the President and, in accordance with that direction, carried out under the authority of the heads of agencies that operate or exercise authority over such national security systems.

''(d) STATUTORY CONSTRUCTION.—Nothing in this subchapter shall be construed to alter or amend any law regarding the authority of any head of an agency over such agency.

''§ 3554. Agency responsibilities

''(a) IN GENERAL.—The head of each agency shall—

''(1) be responsible for—

''(A) complying with the policies and directives issued under section 3553;

''(B) providing information security protections commensurate with the risk resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by the agency or by a contractor of an agency or other organization on behalf of an agency; and

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(C) complying with the requirements of this subchapter, including—

''(i) information security standards and guidelines promulgated under section 11331 of title 40;

''(ii) for any national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued as directed by the President; and

''(iii) for any non-national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued under section 3553;

''(D) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

''(E) reporting and sharing, for an agency operating or exercising control of a national security system, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for national security systems issued as directed by the President; and

''(F) reporting and sharing, for those agencies operating or exercising control of non-national security systems, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for non-national security systems as prescribed under section 3553(a), including information to assist the entity designated under section 3555(a) with the ongoing security analysis under section 3555;

''(2) ensure that each senior agency official provides information security for the information and information systems that support the operations and assets under the senior agency official's control, including by—

''(A) assessing the risk and impact that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

''(B) determining the level of information security appropriate to protect such information and information systems in accordance with policies and directives issued under section 3553(a), and standards and guidelines promulgated under section 11331 of title 40 for information security classifications and related requirements;

''(C) implementing policies, procedures, and capabilities to reduce risks to an acceptable level in a cost-effective manner;

''(D) actively monitoring the effective implementation of information security controls and techniques; and

''(E) reporting information about information security incidents, cyber threat information, and deterioration of security controls in a timely and adequate manner to the entity designated under section 3553(a)(3) in accordance with paragraph (1);

''(3) assess and maintain the resiliency of information technology systems critical to agency mission and operations;

''(4) designate the agency Inspector General (or an independent entity selected in consultation with the Director and the Council of Inspectors General on Integrity and Efficiency if the agency does not have an Inspector General) to conduct the annual independent evaluation required under section 3556, and allow the agency Inspector General to contract with an independent entity to perform such evaluation;

''(5) delegate to the Chief Information Officer or equivalent (or to a senior agency official who reports to the Chief Information Officer or equivalent)—

''(A) the authority and primary responsibility to implement an agencywide information security program; and

''(B) the authority to provide information security for the information collected and maintained by the agency (or by a contractor, other agency, or other source on behalf of the agency) and for the information systems that support the operations, assets, and mission of the agency (including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency);

''(6) delegate to the appropriate agency official (who is responsible for a particular agency system or subsystem) the responsibility to ensure and enforce compliance with all requirements of the agency's agencywide information security program in coordination with the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5);

''(7) ensure that an agency has trained personnel who have obtained any necessary security clearances to permit them to assist the agency in complying with this subchapter;

''(8) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5), in coordination with other senior agency officials, reports to the agency head on the effectiveness of the agencywide information security program, including the progress of any remedial actions; and

''(9) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5) has the necessary qualifications to administer the functions described in this subchapter and has information security duties as a primary duty of that official.

''(b) CHIEF INFORMATION OFFICERS.—Each Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under subsection (a)(5) shall—

''(1) establish and maintain an enterprise security operations capability that on a continuous basis—

''(A) detects, reports, contains, mitigates, and responds to information security incidents that impair adequate security of the agency's information or information system in a timely manner and in accordance with the policies and directives under section 3553; and

''(B) reports any information security incident under subparagraph (A) to the entity designated under section 3555;

''(2) develop, maintain, and oversee an agencywide information security program;

''(3) develop, maintain, and oversee information security policies, procedures, and control techniques to address applicable requirements, including requirements under section 3553 of this title and section 11331 of title 40; and

''(4) train and oversee the agency personnel who have significant responsibility for information security with respect to that responsibility.

''(c) AGENCYWIDE INFORMATION SECURITY PROGRAMS.—

''(1) IN GENERAL.—Each agencywide information security program under subsection (b)(2) shall include—

''(A) relevant security risk assessments, including technical assessments and others related to the acquisition process;

''(B) security testing commensurate with risk and impact;

''(C) mitigation of deterioration of security controls commensurate with risk and impact;

''(D) risk-based continuous monitoring and threat assessment of the operational status and security of agency information systems to enable evaluation of the effectiveness of and compliance with information security policies, procedures, and practices, including a relevant and appropriate selection of security controls of information systems identified in the inventory under section 3505(c);

''(E) operation of appropriate technical capabilities in order to detect, mitigate, report, and respond to information security incidents, cyber threat information, and deterioration of security controls in a manner that is consistent with the policies and directives under section 3553, including—

''(i) mitigating risks associated with such information security incidents;

''(ii) notifying and consulting with the entity designated under section 3555; and

''(iii) notifying and consulting with, as appropriate—

''(I) law enforcement and the relevant Office of the Inspector General; and

''(II) any other entity, in accordance with law and as directed by the President;

''(F) a process to ensure that remedial action is taken to address any deficiencies in the information security policies, procedures, and practices of the agency; and

''(G) a plan and procedures to ensure the continuity of operations for information systems that support the operations and assets of the agency.

''(2) RISK MANAGEMENT STRATEGIES.—Each agencywide information security program under subsection (b)(2) shall include the development and maintenance of a risk management strategy for information security. The risk management strategy shall include—

''(A) consideration of information security incidents, cyber threat information, and deterioration of security controls; and

''(B) consideration of the consequences that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency;

''(3) POLICIES AND PROCEDURES.—Each agencywide information security program under subsection (b)(2) shall include policies and procedures that—

''(A) are based on the risk management strategy under paragraph (2);

''(B) reduce information security risks to an acceptable level in a cost-effective manner;

''(C) ensure that cost-effective and adequate information security is addressed as part of the acquisition and ongoing management of each agency information system; and

''(D) ensure compliance with—

''(i) this subchapter; and

''(ii) any other applicable requirements.

''(4) TRAINING REQUIREMENTS.—Each agencywide information security program under subsection (b)(2) shall include information security, privacy, civil rights, civil liberties, and information oversight training that meets any applicable requirements under section 3553. The training shall inform each information security personnel that has access to agency information systems (including contractors and other users of information systems that support the operations and assets of the agency) of—

''(A) the information security risks associated with the information security personnel's activities; and

''(B) the individual's responsibility to comply with the agency policies and procedures that reduce the risks under subparagraph (A).

''(d) ANNUAL REPORT.—Each agency shall submit a report annually to the Secretary of Homeland Security on its agencywide information security program and information systems.

''§ 3555. Multiagency ongoing threat assessment

''(a) IMPLEMENTATION.—The Director of the Office of Management and Budget, in coordination with the Secretary of Homeland Security, shall designate an entity to implement ongoing security analysis concerning agency information systems—

''(1) based on cyber threat information;

''(2) based on agency information system and environment of operation changes, including—

''(A) an ongoing evaluation of the information system security controls; and

''(B) the security state, risk level, and environment of operation of an agency information system, including—

''(i) a change in risk level due to a new cyber threat;

''(ii) a change resulting from a new technology;

''(iii) a change resulting from the agency's mission; and

''(iv) a change resulting from the business practice; and

''(3) using automated processes to the maximum extent possible—

''(A) to increase information system security;

''(B) to reduce paper-based reporting requirements; and

''(C) to maintain timely and actionable knowledge of the state of the information system security.

''(b) STANDARDS.—The National Institute of Standards and Technology may promulgate standards, in coordination with the Secretary of Homeland Security, to assist an agency with its duties under this section.

''(c) COMPLIANCE.—The head of each appropriate department and agency shall be responsible for ensuring compliance and implementing necessary procedures to comply with this section. The head of each appropriate department and agency, in consultation with the Director of the Office of Management and Budget and the Secretary of Homeland Security, shall—

''(1) monitor compliance under this section;

''(2) develop a timeline and implement for the department or agency—

''(A) adoption of any technology, system, or method that facilitates continuous monitoring and threat assessments of an agency information system;

''(B) adoption or updating of any technology, system, or method that prevents, detects, or remediates a significant cyber incident to a Federal information system of the department or agency that has impeded, or is reasonably likely to impede, the performance of a critical mission of the department or agency; and

''(C) adoption of any technology, system, or method that satisfies a requirement under this section.

''(d) LIMITATION OF AUTHORITY.—The authorities of the Director of the Office of Management and Budget and of the Secretary of Homeland Security under this section shall not apply to national security systems.

''(e) REPORT.—Not later than 6 months after the date of enactment of the Cybersecurity Act of 2012, the Government Accountability Office shall issue a report evaluating each agency's status toward implementing this section.

''§ 3556. Independent evaluations

''(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency, in consultation with the Director and the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense, shall issue and maintain criteria for the timely, cost-effective, risk-based, and independent evaluation of each agencywide information security program (and practices) to determine the effectiveness of the agencywide information security program (and practices). The criteria shall include measures to assess any conflicts of interest in the performance of the evaluation and whether the agencywide information security program includes appropriate safeguards against disclosure of information where such disclosure may adversely affect information security.

''(b) ANNUAL INDEPENDENT EVALUATIONS.—Each agency shall perform an annual independent evaluation of its agencywide information security program (and practices) in accordance with the criteria under subsection (a).

''(c) DISTRIBUTION OF REPORTS.—Not later than 30 days after receiving an independent evaluation under subsection (b), each agency head shall transmit a copy of the independent evaluation to the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense.

''(d) NATIONAL SECURITY SYSTEMS.—Evaluations involving national security systems shall be conducted as directed by President.

''§ 3557. National security systems.

''The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

''(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system; and

''(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President.''.

(b) SAVINGS PROVISIONS.—

(1) POLICY AND COMPLIANCE GUIDANCE.—Policy and compliance guidance issued by the Director before the date of enactment of this Act under section 3543(a)(1) of title 44, United States Code (as in effect on the day before the date of enactment of this Act), shall continue in effect, according to its terms, until modified, terminated, superseded, or repealed pursuant to section 3553(a)(1) of title 44, United States Code.

(2) STANDARDS AND GUIDELINES.—Standards and guidelines issued by the Secretary of Commerce or by the Director before the date of enactment of this Act under section 11331(a)(1) of title 40, United States Code, (as in effect on the day before the date of enactment of this Act) shall continue in effect, according to their terms, until modified, terminated, superseded, or repealed pursuant to section 11331(a)(1) of title 40, United States Code, as amended by this Act.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) CHAPTER ANALYSIS.—The chapter analysis for chapter 35 of title 44, United States Code, is amended—

(A) by striking the items relating to sections 3531 through 3538;

(B) by striking the items relating to sections 3541 through 3549; and

(C) by inserting the following:

''3551. Purposes.
''3552. Definitions.
''3553. Federal information security authority and coordination.
''3554. Agency responsibilities.
''3555. Multiagency ongoing threat assessment.
''3556. Independent evaluations.
''3557. National security systems.''.

(2) OTHER REFERENCES.—

(A) Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(1)(A)) is amended by striking ''section 3532(3)'' and inserting ''section 3552''.

(B) Section 2222(j)(5) of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(C) Section 2223(c)(3) of title 10, United States Code, is amended, by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(D) Section 2315 of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(E) Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended—

(i) in subsection (a)(2), by striking ''section 3532(b)(2)'' and inserting ''section 3552'';

(ii) in subsection (c)(3), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iii) in subsection (d)(1), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iv) in subsection (d)(8) by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(v) in subsection (d)(8), by striking ''submitted to the Director'' and inserting ''submitted to the Secretary'';

(vi) in subsection (e)(2), by striking ''section 3532(1) of such title'' and inserting ''section 3552 of title 44''; and

(vii) in subsection (e)(5), by striking ''section 3532(b)(2) of such title'' and inserting ''section 3552 of title 44''.

(F) Section 8(d)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7406(d)(1)) is amended by striking ''section 3534(b)'' and inserting ''section 3554(b)(2)''.

SEC. 302. MANAGEMENT OF INFORMATION TECHNOLOGY.

(a) IN GENERAL.—Section 11331 of title 40, United States Code, is amended to read as follows:

''§ 11331. Responsibilities for Federal information systems standards

''(a) STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO PRESCRIBE.—Except as provided under paragraph (2), the Secretary of Commerce shall prescribe standards and guidelines pertaining to Federal information systems—

''(A) in consultation with the Secretary of Homeland Security; and

''(B) on the basis of standards and guidelines developed by the National Institute of Standards and Technology under paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)(2) and (a)(3)).

''(2) NATIONAL SECURITY SYSTEMS.—Standards and guidelines for national security systems shall be developed, prescribed, enforced, and overseen as otherwise authorized by law and as directed by the President.

''(b) MANDATORY STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO MAKE MANDATORY STANDARDS AND GUIDELINES.—The Secretary of Commerce shall make standards and guidelines under subsection (a)(1) compulsory and binding to the extent determined necessary by the Secretary of Commerce to improve the efficiency of operation or security of Federal information systems.

''(2) REQUIRED MANDATORY STANDARDS AND GUIDELINES.—

''(A) IN GENERAL.—Standards and guidelines under subsection (a)(1) shall include information security standards that—

''(i) provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)); and

''(ii) are otherwise necessary to improve the security of Federal information and information systems.

''(B) BINDING EFFECT.—Information security standards under subparagraph (A) shall be compulsory and binding.

''(c) EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary of Commerce shall exercise the authority conferred by this section subject to direction by the President and in coordination with the Director.

''(d) APPLICATION OF MORE STRINGENT STANDARDS AND GUIDELINES.—The head of an executive agency may employ standards for the cost-effective information security for information systems within or under the supervision of that agency that are more stringent than the standards and guidelines the Secretary of Commerce prescribes under this section if the more stringent standards and guidelines—

''(1) contain at least the applicable standards and guidelines made compulsory and binding by the Secretary of Commerce; and

''(2) are otherwise consistent with the policies, directives, and implementation memoranda issued under section 3553(a) of title 44.

''(e) DECISIONS ON PROMULGATION OF STANDARDS AND GUIDELINES.—The decision by the Secretary of Commerce regarding the promulgation of any standard or guideline under this section shall occur not later than 6 months after the date of submission of the proposed standard to the Secretary of Commerce by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

''(f) NOTICE AND COMMENT.—A decision by the Secretary of Commerce to significantly modify, or not promulgate, a proposed standard submitted to the Secretary by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) shall be made after the public is given an opportunity to comment on the Secretary's proposed decision.

''(g) DEFINITIONS.—In this section:

''(1) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' has the meaning given the term in section 3552 of title 44.

''(2) INFORMATION SECURITY.—The term 'information security' has the meaning given the term in section 3552 of title 44.

''(3) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given the term in section 3552 of title 44.''.

SEC. 303. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 304. TECHNICAL AND CONFORMING AMENDMENTS.

Section 21(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4(b)) is amended—

(1) in paragraph (2), by striking ''and the Director of the Office of Management and Budget'' and inserting '', the Secretary of Commerce, and the Secretary of Homeland Security''; and

(2) in paragraph (3), by inserting '', the Secretary of Homeland Security,'' after ''the Secretary of Commerce''.

SEC. 305. CLARIFICATION OF AUTHORITIES.

Nothing in this title shall be construed to convey any new regulatory authority to any government entity implementing or complying with any provision of this title.

TITLE IV—CRIMINAL PENALTIES

SEC. 401. PENALTIES FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030(c) of title 18, United States Code, is amended to read as follows:

''(c) The punishment for an offense under subsection (a) or (b) of this section is—

''(1) a fine under this title or imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(1) of this section;

''(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than 3 years, or both, in the case of an offense under subsection (a)(2); or

''(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2) of this section, if—

''(i) the offense was committed for purposes of commercial advantage or private financial gain;

''(ii) the offense was committed in the furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States, or of any State; or

''(iii) the value of the information obtained, or that would have been obtained if the offense was completed, exceeds $5,000;

''(3) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(3) of this section;

''(4) a fine under this title or imprisonment of not more than 20 years, or both, in the case of an offense under subsection (a)(4) of this section;

''(5)(A) except as provided in subparagraph (C), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A) of this section, if the offense caused—

''(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

''(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

''(iii) physical injury to any person;

''(iv) a threat to public health or safety;

''(v) damage affecting a computer used by, or on behalf of, an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

''(vi) damage affecting 10 or more protected computers during any 1-year period;

''(B) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(B), if the offense caused a harm provided in clause (i) through (vi) of subparagraph (A) of this subsection;

''(C) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both;

''(D) a fine under this title, imprisonment for not more than 10 years, or both, for any other offense under subsection (a)(5);

''(E) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(6) of this section; or

''(F) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(7) of this section.''.

SEC. 402. TRAFFICKING IN PASSWORDS.

Section 1030(a)(6) of title 18, United States Code, is amended to read as follows:

''(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information or means of access through which a protected computer (as defined in subparagraphs (A) and (B) of subsection (e)(2)) may be accessed without authorization.''.

SEC. 403. CONSPIRACY AND ATTEMPTED COMPUTER FRAUD OFFENSES.

Section 1030(b) of title 18, United States Code, is amended by inserting ''as if for the completed offense'' after ''punished as provided''.

SEC. 404. CRIMINAL AND CIVIL FORFEITURE FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030 of title 18, United States Code, is amended by striking subsections (i) and (j) and inserting the following:

''(i) CRIMINAL FORFEITURE.—

''(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

''(A) such persons interest in any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of such violation; and

''(B) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of such violation.

''(2) The criminal forfeiture of property under this subsection, including any seizure and disposition of the property, and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

''(j) CIVIL FORFEITURE.—

''(1) The following shall be subject to forfeiture to the United States and no property right, real or personal, shall exist in them:

''(A) Any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of any violation of this section, or a conspiracy to violate this section.

''(B) Any property, real or personal, constituting or derived from any gross proceeds obtained directly or indirectly, or any property traceable to such property, as a result of the commission of any violation of this section, or a conspiracy to violate this section.

''(2) Seizures and forfeitures under this subsection shall be governed by the provisions in chapter 46 relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents and other persons as may be designated for that purpose by the Secretary of Homeland Security or the Attorney General.''.

SEC. 405. DAMAGE TO CRITICAL INFRASTRUCTURE COMPUTERS.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

''§ 1030A. Aggravated damage to a critical infrastructure computer

''(a) DEFINITIONS.—In this section—

''(1) the term 'computer' has the meaning given the term in section 1030;

''(2) the term 'critical infrastructure computer' means a computer that manages or controls systems or assets vital to national defense, national security, national economic security, public health or safety, or any combination of those matters, whether publicly or privately owned or operated, including—

''(A) oil and gas production, storage, conversion, and delivery systems;

''(B) water supply systems;

''(C) telecommunication networks;

''(D) electrical power generation and delivery systems;

''(E) finance and banking systems;

''(F) emergency services;

''(G) transportation systems and services; and

''(H) government operations that provide essential services to the public; and

''(3) the term 'damage' has the meaning given the term in section 1030.

''(b) OFFENSE.—It shall be unlawful, during and in relation to a felony violation of section 1030, to knowingly cause or attempt to cause damage to a critical infrastructure computer if the damage results in (or, in the case of an attempt, if completed, would have resulted in) the substantial impairment—

''(1) of the operation of the critical infrastructure computer; or

''(2) of the critical infrastructure associated with the computer.

''(c) PENALTY.—Any person who violates subsection (b) shall be—

''(1) fined under this title;

''(2) imprisoned for not less than 3 years but not more than 20 years; or

''(3) penalized under paragraphs (1) and (2).

''(d) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

''(1) a court shall not place on probation any person convicted of a violation of this section;

''(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment, including any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for a felony violation of section 1030;

''(3) in determining any term of imprisonment to be imposed for a felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The chapter analysis for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

''1030A. Aggravated damage to a critical infrastructure computer.''.

SEC. 406. LIMITATION ON ACTIONS INVOLVING UNAUTHORIZED USE.

Section 1030(e)(6) of title 18, United States Code, is amended by striking ''alter;'' and inserting ''alter, but does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized;''.

SEC. 407. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

TITLE V—CYBERSECURITY RESEARCH AND DEVELOPMENT

SEC. 501. NATIONAL HIGH-PERFORMANCE COMPUTING PROGRAM PLANNING AND COORDINATION.

(a) GOALS AND PRIORITIES.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(d) GOALS AND PRIORITIES.—The goals and priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include—

''(1) encouraging and supporting mechanisms for interdisciplinary research and development in networking and information technology, including—

''(A) through collaborations across agencies;

''(B) through collaborations across Program Component Areas;

''(C) through collaborations with industry;

''(D) through collaborations with institutions of higher education;

''(E) through collaborations with Federal laboratories (as defined in section 4 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3703)); and

''(F) through collaborations with international organizations;

''(2) addressing national, multi-agency, multi-faceted challenges of national importance; and

''(3) fostering the transfer of research and development results into new technologies and applications for the benefit of society.''.

(b) DEVELOPMENT OF STRATEGIC PLAN.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(e) STRATEGIC PLAN.—

''(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Cybersecurity Act of 2012, the agencies under subsection (a)(3)(B), working through the National Science and Technology Council and with the assistance of the Office of Science and Technology Policy shall develop a 5-year strategic plan to guide the activities under subsection (a)(1).

''(2) CONTENTS.—The strategic plan shall specify—

''(A) the near-term objectives for the Program;

''(B) the long-term objectives for the Program;

''(C) the anticipated time frame for achieving the near-term objectives;

''(D) the metrics that will be used to assess any progress made toward achieving the near-term objectives and the long-term objectives; and

''(E) how the Program will achieve the goals and priorities under subsection (d).

''(3) IMPLEMENTATION ROADMAP.—

''(A) IN GENERAL.—The agencies under subsection (a)(3)(B) shall develop and annually update an implementation roadmap for the strategic plan.

''(B) REQUIREMENTS.—The information in the implementation roadmap shall be coordinated with the database under section 102(c) and the annual report under section 101(a)(3). The implementation roadmap shall—

''(i) specify the role of each Federal agency in carrying out or sponsoring research and development to meet the research objectives of the strategic plan, including a description of how progress toward the research objectives will be evaluated, with consideration of any relevant recommendations of the advisory committee;

''(ii) specify the funding allocated to each major research objective of the strategic plan and the source of funding by agency for the current fiscal year; and

''(iii) estimate the funding required for each major research objective of the strategic plan for the next 3 fiscal years.

''(4) RECOMMENDATIONS.—The agencies under subsection (a)(3)(B) shall take into consideration when developing the strategic plan under paragraph (1) the recommendations of—

''(A) the advisory committee under subsection (b); and

''(B) the stakeholders under section 102(a)(3).

''(5) REPORT TO CONGRESS.—The Director of the Office of Science and Technology Policy shall transmit the strategic plan under this subsection, including the implementation roadmap and any updates under paragraph (3), to—

''(A) the advisory committee under subsection (b);

''(B) the Committee on Commerce, Science, and Transportation of the Senate; and

''(C) the Committee on Science and Technology of the House of Representatives.''.

(c) PERIODIC REVIEWS.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(f) PERIODIC REVIEWS.—The agencies under subsection (a)(3)(B) shall—

''(1) periodically assess the contents and funding levels of the Program Component Areas and restructure the Program when warranted, taking into consideration any relevant recommendations of the advisory committee under subsection (b); and

''(2) ensure that the Program includes national, multi-agency, multi-faceted research and development activities, including activities described in section 104.''.

(d) ADDITIONAL RESPONSIBILITIES OF DIRECTOR.—Section 101(a)(2) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(2)) is amended—

(1) by redesignating subparagraphs (E) and (F) as subparagraphs (G) and (H), respectively; and

(2) by inserting after subparagraph (D) the following:

''(E) encourage and monitor the efforts of the agencies participating in the Program to allocate the level of resources and management attention necessary—

''(i) to ensure that the strategic plan under subsection (e) is developed and executed effectively; and

''(ii) to ensure that the objectives of the Program are met;

''(F) working with the Office of Management and Budget and in coordination with the creation of the database under section 102(c), direct the Office of Science and Technology Policy and the agencies participating in the Program to establish a mechanism (consistent with existing law) to track all ongoing and completed research and development projects and associated funding;''.

(e) ADVISORY COMMITTEE.—Section 101(b) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(b)) is amended—

(1) in paragraph (1)—

(A) by inserting after the first sentence the following: ''The co-chairs of the advisory committee shall meet the qualifications of committee members and may be members of the Presidents Council of Advisors on Science and Technology.''; and

(B) by striking ''high-performance'' in subparagraph (D) and inserting ''high-end''; and

(2) by amending paragraph (2) to read as follows:

''(2) In addition to the duties under paragraph (1), the advisory committee shall conduct periodic evaluations of the funding, management, coordination, implementation, and activities of the Program. The advisory committee shall report its findings and recommendations not less frequently than once every 3 fiscal years to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives. The report shall be submitted in conjunction with the update of the strategic plan.''.

(f) REPORT.—Section 101(a)(3) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(3)) is amended—

(1) in subparagraph (C)—

(A) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(B) by striking ''each Program Component Area'' and inserting ''each Program Component Area and each research area supported in accordance with section 104'';

(2) in subparagraph (D)—

(A) by striking ''each Program Component Area,'' and inserting ''each Program Component Area and each research area supported in accordance with section 104,'';

(B) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(C) by striking ''and'' after the semicolon;

(3) by redesignating subparagraph (E) as subparagraph (G); and

(4) by inserting after subparagraph (D) the following:

''(E) include a description of how the objectives for each Program Component Area, and the objectives for activities that involve multiple Program Component Areas, relate to the objectives of the Program identified in the strategic plan under subsection (e);

''(F) include—

''(i) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the next fiscal year by category of activity;

''(ii) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the current fiscal year by category of activity; and

''(iii) the amount of funding provided for the Office of Science and Technology Policy for the current fiscal year by each agency participating in the Program; and''.

(g) DEFINITIONS.—Section 4 of the High-Performance Computing Act of 1991 (15 U.S.C. 5503) is amended—

(1) by redesignating paragraphs (1) and (2) as paragraphs (2) and (3), respectively;

(2) by redesignating paragraph (3) as paragraph (6);

(3) by redesignating paragraphs (6) and (7) as paragraphs (7) and (8), respectively;

(4) by inserting before paragraph (2), as redesignated, the following:

''(1) 'cyber-physical systems' means physical or engineered systems whose networking and information technology functions and physical elements are deeply integrated and are actively connected to the physical world through sensors, actuators, or other means to perform monitoring and control functions;'';

(5) in paragraph (3), as redesignated, by striking ''high-performance computing'' and inserting ''networking and information technology'';

(6) in paragraph (6), as redesignated—

(A) by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(B) by striking ''supercomputer'' and inserting ''high-end computing'';

(7) in paragraph (5), by striking ''network referred to as'' and all that follows through the semicolon and inserting ''network, including advanced computer networks of Federal agencies and departments''; and

(8) in paragraph (7), as redesignated, by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program''.

SEC. 502. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

(a) RESEARCH IN AREAS OF NATIONAL IMPORTANCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.) is amended by adding at the end the following:

''SEC. 104. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

''(a) IN GENERAL.—The Program shall encourage agencies under section 101(a)(3)(B) to support, maintain, and improve national, multi-agency, multi-faceted, research and development activities in networking and information technology directed toward application areas that have the potential for significant contributions to national economic competitiveness and for other significant societal benefits.

''(b) TECHNICAL SOLUTIONS.—An activity under subsection (a) shall be designed to advance the development of research discoveries by demonstrating technical solutions to important problems in areas including—

''(1) cybersecurity;

''(2) health care;

''(3) energy management and low-power systems and devices;

''(4) transportation, including surface and air transportation;

''(5) cyber-physical systems;

''(6) large-scale data analysis and modeling of physical phenomena;

''(7) large scale data analysis and modeling of behavioral phenomena;

''(8) supply chain quality and security; and

''(9) privacy protection and protected disclosure of confidential data.

''(c) RECOMMENDATIONS.—The advisory committee under section 101(b) shall make recommendations to the Program for candidate research and development areas for support under this section.

''(d) CHARACTERISTICS.—

''(1) IN GENERAL.—Research and development activities under this section—

''(A) shall include projects selected on the basis of applications for support through a competitive, merit-based process;

''(B) shall leverage, when possible, Federal investments through collaboration with related State initiatives;

''(C) shall include a plan for fostering the transfer of research discoveries and the results of technology demonstration activities, including from institutions of higher education and Federal laboratories, to industry for commercial development;

''(D) shall involve collaborations among researchers in institutions of higher education and industry; and

''(E) may involve collaborations among nonprofit research institutions and Federal laboratories, as appropriate.

''(2) COST-SHARING.—In selecting applications for support, the agencies under section 101(a)(3)(B) shall give special consideration to projects that include cost sharing from non-Federal sources.

''(3) MULTIDISCIPLINARY RESEARCH CENTERS.—Research and development activities under this section shall be supported through multidisciplinary research centers, including Federal laboratories, that are organized to investigate basic research questions and carry out technology demonstration activities in areas described in subsection (a). Research may be carried out through existing multidisciplinary centers, including those authorized under section 7024(b)(2) of the America COMPETES Act (42 U.S.C. 1862o–10(2)).''.

(b) CYBER-PHYSICAL SYSTEMS.—Section 101(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following:

''(J) provide for increased understanding of the scientific principles of cyber-physical systems and improve the methods available for the design, development, and operation of cyber-physical systems that are characterized by high reliability, safety, and security; and

''(K) provide for research and development on human-computer interactions, visualization, and big data.''.

(c) TASK FORCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.), as amended by section 502(a) of this Act, is amended by adding at the end the following:

''SEC. 105. TASK FORCE.

''(a) ESTABLISHMENT.—Not later than 180 days after the date of enactment the Cybersecurity Act of 2012, the Director of the Office of Science and Technology Policy under section 102 shall convene a task force to explore mechanisms for carrying out collaborative research and development activities for cyber-physical systems (including the related technologies required to enable these systems) through a consortium or other appropriate entity with participants from institutions of higher education, Federal laboratories, and industry.

''(b) FUNCTIONS.—The task force shall—

''(1) develop options for a collaborative model and an organizational structure for such entity under which the joint research and development activities could be planned, managed, and conducted effectively, including mechanisms for the allocation of resources among the participants in such entity for support of such activities;

''(2) propose a process for developing a research and development agenda for such entity, including guidelines to ensure an appropriate scope of work focused on nationally significant challenges and requiring collaboration and to ensure the development of related scientific and technological milestones;

''(3) define the roles and responsibilities for the participants from institutions of higher education, Federal laboratories, and industry in such entity;

''(4) propose guidelines for assigning intellectual property rights and for transferring research results to the private sector; and

''(5) make recommendations for how such entity could be funded from Federal, State, and non-governmental sources.

''(c) COMPOSITION.—In establishing the task force under subsection (a), the Director of the Office of Science and Technology Policy shall appoint an equal number of individuals from institutions of higher education and from industry with knowledge and expertise in cyber-physical systems, and may appoint not more than 2 individuals from Federal laboratories.

''(d) REPORT.—Not later than 1 year after the date of enactment of the Cybersecurity Act of 2012, the Director of the Office of Science and Technology Policy shall transmit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives a report describing the findings and recommendations of the task force.

''(e) TERMINATION.—The task force shall terminate upon transmittal of the report required under subsection (d).

''(f) COMPENSATION AND EXPENSES.—Members of the task force shall serve without compensation.''.

SEC. 503. PROGRAM IMPROVEMENTS.

Section 102 of the High-Performance Computing Act of 1991 (15 U.S.C. 5512) is amended to read as follows:

''SEC. 102. PROGRAM IMPROVEMENTS.

''(a) FUNCTIONS.—The Director of the Office of Science and Technology Policy shall continue—

''(1) to provide technical and administrative support to—

''(A) the agencies participating in planning and implementing the Program, including support needed to develop the strategic plan under section 101(e); and

''(B) the advisory committee under section 101(b);

''(2) to serve as the primary point of contact on Federal networking and information technology activities for government agencies, academia, industry, professional societies, State computing and networking technology programs, interested citizen groups, and others to exchange technical and programmatic information;

''(3) to solicit input and recommendations from a wide range of stakeholders during the development of each strategic plan under section 101(e) by convening at least 1 workshop with invitees from academia, industry, Federal laboratories, and other relevant organizations and institutions;

''(4) to conduct public outreach, including the dissemination of the advisory committee's findings and recommendations, as appropriate;

''(5) to promote access to and early application of the technologies, innovations, and expertise derived from Program activities to agency missions and systems across the Federal Government and to United States industry;

''(6) to ensure accurate and detailed budget reporting of networking and information technology research and development investment; and

''(7) to encourage agencies participating in the Program to use existing programs and resources to strengthen networking and information technology education and training, and increase participation in such fields, including by women and underrepresented minorities.

''(b) SOURCE OF FUNDING.—

''(1) IN GENERAL.—The functions under this section shall be supported by funds from each agency participating in the Program.

''(2) SPECIFICATIONS.—The portion of the total budget of the Office of Science and Technology Policy that is provided by each agency participating in the Program for each fiscal year shall be in the same proportion as each agency's share of the total budget for the Program for the previous fiscal year, as specified in the database under section 102(c).

''(c) DATABASE.—

''(1) IN GENERAL.—The Director of the Office of Science and Technology Policy shall develop and maintain a database of projects funded by each agency for the fiscal year for each Program Component Area.

''(2) PUBLIC ACCESSIBILITY.—The Director of the Office of Science and Technology Policy shall make the database accessible to the public.

''(3) DATABASE CONTENTS.—The database shall include, for each project in the database—

''(A) a description of the project;

''(B) each agency, industry, institution of higher education, Federal laboratory, or international institution involved in the project;

''(C) the source funding of the project (set forth by agency);

''(D) the funding history of the project; and

''(E) whether the project has been completed.''.

SEC. 504. IMPROVING EDUCATION OF NETWORKING AND INFORMATION TECHNOLOGY, INCLUDING HIGH PERFORMANCE COMPUTING.

Section 201(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)) is amended—

(1) by redesignating paragraphs (2) through (4) as paragraphs (3) through (5), respectively; and

(2) by inserting after paragraph (1) the following:

''(2) the National Science Foundation shall use its existing programs, in collaboration with other agencies, as appropriate, to improve the teaching and learning of networking and information technology at all levels of education and to increase participation in networking and information technology fields;''.

SEC. 505. CONFORMING AND TECHNICAL AMENDMENTS TO THE HIGH-PERFORMANCE COMPUTING ACT OF 1991.

(a) SECTION 3.—Section 3 of the High-Performance Computing Act of 1991 (15 U.S.C. 5502) is amended—

(1) in the matter preceding paragraph (1), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(2) in paragraph (1)—

(A) in the matter preceding subparagraph (A), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(B) in subparagraphs (A), (F), and (G), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(C) in subparagraph (H), by striking ''high-performance'' and inserting ''high-end''; and

(3) in paragraph (2)—

(A) by striking ''high-performance computing and'' and inserting ''networking and information technology, and''; and

(B) by striking ''high-performance computing network'' and inserting ''networking and information technology''.

(b) TITLE HEADING.—The heading of title I of the High-Performance Computing Act of 1991 (105 Stat. 1595) is amended by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''.

(c) SECTION 101.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT**'';

(2) in subsection (a)—

(A) in the subsection heading, by striking ''NATIONAL HIGH-PERFORMANCE COMPUTING'' and inserting ''NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT'';

(B) in paragraph (1)—

(i) by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program'';

(ii) in subparagraph (A), by striking ''high-performance computing, including networking'' and inserting ''networking and information technology'';

(iii) in subparagraphs (B) and (G), by striking ''high-performance'' each place it appears and inserting ''high-end''; and

(iv) in subparagraph (C), by striking ''high-performance computing and networking'' and inserting ''high-end computing, distributed, and networking''; and

(C) in paragraph (2)—

(i) in subparagraphs (A) and (C)—

(I) by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(II) by striking ''development, networking,'' each place it appears and inserting ''development,''; and

(ii) in subparagraphs (G) and (H), as redesignated by section 501(d) of this Act, by striking ''high-performance'' each place it appears and inserting ''high-end'';

(3) in subsection (b)(1), in the matter preceding subparagraph (A), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(4) in subsection (c)(1)(A), by striking ''high-performance computing'' and inserting ''networking and information technology''.

(d) SECTION 201.—Section 201(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)(1)) is amended by striking ''high-performance computing and advanced high-speed computer networking'' and inserting ''networking and information technology research and development''.

(e) SECTION 202.—Section 202(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5522(a)) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(f) SECTION 203.—Section 203(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5523(a)) is amended—

(1) in paragraph (1), by striking ''high-performance computing and networking'' and inserting ''networking and information technology''; and

(2) in paragraph (2)(A), by striking ''high-performance'' and inserting ''high-end''.

(g) SECTION 204.—Section 204 of the High-Performance Computing Act of 1991 (15 U.S.C. 5524) is amended—

(1) in subsection (a)(1)—

(A) in subparagraph (A), by striking ''high-performance computing systems and networks'' and inserting ''networking and information technology systems and capabilities'';

(B) in subparagraph (B), by striking ''interoperability of high-performance computing systems in networks and for common user interfaces to systems'' and inserting ''interoperability and usability of networking and information technology systems''; and

(C) in subparagraph (C), by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(2) in subsection (b)—

(A) by striking ''HIGH-PERFORMANCE COMPUTING AND NETWORK'' in the heading and inserting ''NETWORKING AND INFORMATION TECHNOLOGY''; and

(B) by striking ''sensitive''.

(h) SECTION 205.—Section 205(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5525(a)) is amended by striking ''computational'' and inserting ''networking and information technology''.

(i) SECTION 206.—Section 206(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5526(a)) is amended by striking ''computational research'' and inserting ''networking and information technology research''.

(j) SECTION 207.—Section 207 of the High-Performance Computing Act of 1991 (15 U.S.C. 5527) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(k) SECTION 208.—Section 208 of the High-Performance Computing Act of 1991 (15 U.S.C. 5528) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''; and

(2) in subsection (a)—

(A) in paragraph (1), by striking ''High-performance computing and associated'' and inserting ''Networking and information'';

(B) in paragraph (2), by striking ''high-performance computing'' and inserting ''networking and information technologies'';

(C) in paragraph (3), by striking ''high-performance'' and inserting ''high-end'';

(D) in paragraph (4), by striking ''high-performance computers and associated'' and inserting ''networking and information''; and

(E) in paragraph (5), by striking ''high-performance computing and associated'' and inserting ''networking and information''.

SEC. 506. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation, in coordination with the Secretary of Homeland Security, shall carry out a Federal cyber scholarship-for-service program to recruit and train the next generation of information technology professionals and security managers to meet the needs of the cybersecurity mission for the Federal government.

(b) PROGRAM DESCRIPTION AND COMPONENTS.—The program shall—

(1) annually assess the workforce needs of the Federal government for cybersecurity professionals, including network engineers, software engineers, and other experts in order to determine how many scholarships should be awarded annually to ensure that the workforce needs following graduation match the number of scholarships awarded;

(2) provide scholarships for up to 1,000 students per year in their pursuit of undergraduate or graduate degrees in the cybersecurity field, in an amount that may include coverage for full tuition, fees, and a stipend;

(3) require each scholarship recipient, as a condition of receiving a scholarship under the program, to serve in a Federal information technology workforce for a period equal to one and one-half times each year, or partial year, of scholarship received, in addition to an internship in the cybersecurity field, if applicable, following graduation;

(4) provide a procedure for the National Science Foundation or a Federal agency, consistent with regulations of the Office of Personnel Management, to request and fund a security clearance for a scholarship recipient, including providing for clearance during a summer internship and upon graduation; and

(5) provide opportunities for students to receive temporary appointments for meaningful employment in the Federal information technology workforce during school vacation periods and for internships.

(c) HIRING AUTHORITY.—

(1) IN GENERAL.—For purposes of any law or regulation governing the appointment of an individual in the Federal civil service, upon the successful completion of the student's studies, a student receiving a scholarship under the program may—

(A) be hired under section 213.3102(r) of title 5, Code of Federal Regulations; and

(B) be exempt from competitive service.

(2) COMPETITIVE SERVICE.—Upon satisfactory fulfillment of the service term under paragraph (1), an individual may be converted to a competitive service position without competition if the individual meets the requirements for that position.

(d) ELIGIBILITY.—The eligibility requirements for a scholarship under this section shall include that a scholarship applicant—

(1) be a citizen of the United States;

(2) be eligible to be granted a security clearance;

(3) maintain a grade point average of 3.2 or above on a 4.0 scale for undergraduate study or a 3.5 or above on a 4.0 scale for post-graduate study;

(4) demonstrate a commitment to a career in improving the security of the information infrastructure; and

(5) has demonstrated a level of proficiency in math or computer sciences.

(e) FAILURE TO COMPLETE SERVICE OBLIGATION.—

(1) IN GENERAL.—A scholarship recipient under this section shall be liable to the United States under paragraph (2) if the scholarship recipient—

(A) fails to maintain an acceptable level of academic standing in the educational institution in which the individual is enrolled, as determined by the Director;

(B) is dismissed from such educational institution for disciplinary reasons;

(C) withdraws from the program for which the award was made before the completion of such program;

(D) declares that the individual does not intend to fulfill the service obligation under this section;

(E) fails to fulfill the service obligation of the individual under this section; or

(F) loses a security clearance or becomes ineligible for a security clearance.

(2) REPAYMENT AMOUNTS.—

(A) LESS THAN 1 YEAR OF SERVICE.—If a circumstance under paragraph (1) occurs before the completion of 1 year of a service obligation under this section, the total amount of awards received by the individual under this section shall be repaid.

(B) ONE OR MORE YEARS OF SERVICE.—If a circumstance described in subparagraph (D) or (E) of paragraph (1) occurs after the completion of 1 year of a service obligation under this section, the total amount of scholarship awards received by the individual under this section, reduced by the ratio of the number of years of service completed divided by the number of years of service required, shall be repaid.

(f) EVALUATION AND REPORT.—The Director of the National Science Foundation shall—

(1) evaluate the success of recruiting individuals for scholarships under this section and of hiring and retaining those individuals in the public sector workforce, including the annual cost and an assessment of how the program actually improves the Federal workforce; and

(2) periodically report the findings under paragraph (1) to Congress.

(g) AUTHORIZATION OF APPROPRIATIONS.—From amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), the Director may use funds to carry out the requirements of this section for fiscal years 2012 through 2013.

SEC. 507. STUDY AND ANALYSIS OF CERTIFICATION AND TRAINING OF INFORMATION INFRASTRUCTURE PROFESSIONALS.

(a) STUDY.—The President shall enter into an agreement with the National Academies to conduct a comprehensive study of government, academic, and private-sector accreditation, training, and certification programs for personnel working in information infrastructure. The agreement shall require the National Academies to consult with sector coordinating councils and relevant governmental agencies, regulatory entities, and nongovernmental organizations in the course of the study.

(b) SCOPE.—The study shall include—

(1) an evaluation of the body of knowledge and various skills that specific categories of personnel working in information infrastructure should possess in order to secure information systems;

(2) an assessment of whether existing government, academic, and private-sector accreditation, training, and certification programs provide the body of knowledge and various skills described in paragraph (1);

(3) an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity talent, including barriers relating to compensation, the hiring process, job classification, and hiring flexibility; and

(4) an analysis of the sources and availability of cybersecurity talent, a comparison of the skills and expertise sought by the Federal Government and the private sector, an examination of the current and future capacity of United States institutions of higher education, including community colleges, to provide current and future cybersecurity professionals, through education and training activities, with those skills sought by the Federal Government, State and local entities, and the private sector.

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the National Academies shall submit to the President and Congress a report on the results of the study. The report shall include—

(1) findings regarding the state of information infrastructure accreditation, training, and certification programs, including specific areas of deficiency and demonstrable progress; and

(2) recommendations for the improvement of information infrastructure accreditation, training, and certification programs.

SEC. 508. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

(a) IN GENERAL.—The Director of the National Institute of Standards and Technology, in coordination with appropriate Federal authorities, shall—

(1) as appropriate, ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to Congress a plan for ensuring such Federal agency coordination.

(b) CONSULTATION WITH THE PRIVATE SECTOR.—In carrying out the activities under subsection (a)(1), the Director shall ensure consultation with appropriate private sector stakeholders.

SEC. 509. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

The Director of the National Institute of Standards and Technology shall continue a program to support the development of technical standards, metrology, testbeds, and conformance criteria, taking into account appropriate user concerns—

(1) to improve interoperability among identity management technologies;

(2) to strengthen authentication methods of identity management systems;

(3) to improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols; and

(4) to improve the usability of identity management systems.

SEC. 510. FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY RESEARCH GRANT AREAS.—Section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking ''property.'' and inserting ''property;''; and

(3) by adding at the end the following:

''(J) secure fundamental protocols that are at the heart of inter-network communications and data exchange;

''(K) system security that addresses the building of secure systems from trusted and untrusted components;

''(L) monitoring and detection; and

''(M) resiliency and rapid recovery methods.''.

(b) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY GRANTS.—Section 4(a)(3) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(3)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to

carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(c) COMPUTER AND NETWORK SECURITY CENTERS.—Section 4(b)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7403(b)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(d) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—Section 5(a)(6) of the Cyber Security Research and Development Act (15 U.S.C. 7404(a)(6)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT GRANTS.—Section 5(b)(2) of the Cyber Security Research and Development Act (15 U.S.C. 7404(b)(2)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(f) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY RESEARCH.—Section 5(c)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7404(c)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

SA 2616. Mrs. SHAHEEN (for herself and Mr. PORTMAN) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of the bill, add the following:

TITLE VIII—ENERGY SAVINGS AND INDUSTRIAL COMPETITIVENESS

SEC. 801. SHORT TITLE.

This title may be cited as the ''Energy Savings and Industrial Competitiveness Act of 2012''.

Subtitle A—Buildings

PART I—BUILDING ENERGY CODES

SEC. 811. GREATER ENERGY EFFICIENCY IN BUILDING CODES.

(a) DEFINITIONS.—Section 303 of the Energy Conservation and Production Act (42 U.S.C. 6832) is amended—

(1) by striking paragraph (14) and inserting the following:

''(14) MODEL BUILDING ENERGY CODE.—The term 'model building energy code' means a voluntary building energy code and standards developed and updated through a consensus process among interested persons, such as the IECC or the code used by—

''(A) the Council of American Building Officials;

''(B) the American Society of Heating, Refrigerating, and Air-Conditioning Engineers; or

''(C) other appropriate organizations.''; and

(2) by adding at the end the following:

''(17) IECC.—The term 'IECC' means the International Energy Conservation Code.

''(18) INDIAN TRIBE.—The term 'Indian tribe' has the meaning given the term in section 4 of the Native American Housing Assistance and Self-Determination Act of 1996 (25 U.S.C. 4103).''.

(b) STATE BUILDING ENERGY EFFICIENCY CODES.—Section 304 of the Energy Conservation and Production Act (42 U.S.C. 6833) is amended to read as follows:

''SEC. 304. UPDATING STATE BUILDING ENERGY EFFICIENCY CODES.

''(a) IN GENERAL.—The Secretary shall—

''(1) encourage and support the adoption of building energy codes by States, Indian tribes, and, as appropriate, by local governments that meet or exceed the model building energy codes, or achieve equivalent or greater energy savings; and

''(2) support full compliance with the State and local codes.

''(b) STATE AND INDIAN TRIBE CERTIFICATION OF BUILDING ENERGY CODE UPDATES.—

''(1) REVIEW AND UPDATING OF CODES BY EACH STATE AND INDIAN TRIBE.—

''(A) IN GENERAL.—Not later than 2 years after the date on which a model building energy code is updated, each State or Indian tribe shall certify whether or not the State or Indian tribe, respectively, has reviewed and updated the energy provisions of the building code of the State or Indian tribe, respectively.

''(B) DEMONSTRATION.—The certification shall include a demonstration of whether or not the energy savings for the code provisions that are in effect throughout the State or Indian tribal territory meet or exceed—

''(i) the energy savings of the updated model building energy code; or

''(ii) the targets established under section 307(b)(2).

''(C) NO MODEL BUILDING ENERGY CODE UPDATE.—If a model building energy code is not updated by a target date established under section 307(b)(2)(D), each State or Indian tribe shall, not later than 2 years after the specified date, certify whether or not the State or Indian tribe, respectively, has reviewed and updated the energy provisions of the building code of the State or Indian tribe, respectively, to meet or exceed the target in section 307(b)(2).

''(2) VALIDATION BY SECRETARY.—Not later than 90 days after a State or Indian tribe certification under paragraph (1), the Secretary shall—

''(A) determine whether the code provisions of the State or Indian tribe, respectively, meet the criteria specified in paragraph (1); and

''(B) if the determination is positive, validate the certification.

''(c) IMPROVEMENTS IN COMPLIANCE WITH BUILDING ENERGY CODES.—

''(1) REQUIREMENT.—

''(A) IN GENERAL.—Not later than 3 years after the date of a certification under subsection (b), each State and Indian tribe shall certify whether or not the State and Indian tribe, respectively, has—

''(i) achieved full compliance under paragraph (3) with the applicable certified State and Indian tribe building energy code or with the associated model building energy code; or

''(ii) made significant progress under paragraph (4) toward achieving compliance with the applicable certified State and Indian tribe building energy code or with the associated model building energy code.

''(B) REPEAT CERTIFICATIONS.—If the State or Indian tribe certifies progress toward achieving compliance, the State or Indian tribe shall repeat the certification until the State or Indian tribe certifies that the State or Indian tribe has achieved full compliance, respectively.

''(2) MEASUREMENT OF COMPLIANCE.—A certification under paragraph (1) shall include documentation of the rate of compliance based on—

''(A) independent inspections of a random sample of the buildings covered by the code in the preceding year; or

''(B) an alternative method that yields an accurate measure of compliance.

''(3) ACHIEVEMENT OF COMPLIANCE.—A State or Indian tribe shall be considered to achieve full compliance under paragraph (1) if—

''(A) at least 90 percent of building space covered by the code in the preceding year substantially meets all the requirements of the applicable code specified in paragraph (1), or achieves equivalent or greater energy savings level; or

''(B) the estimated excess energy use of buildings that did not meet the applicable code specified in paragraph (1) in the preceding year, compared to a baseline of comparable buildings that meet this code, is not more than 5 percent of the estimated energy use of all buildings covered by this code during the preceding year.

''(4) SIGNIFICANT PROGRESS TOWARD ACHIEVEMENT OF COMPLIANCE.—A State or Indian tribe shall be considered to have made significant progress toward achieving compliance for purposes of paragraph (1) if the State or Indian tribe—

''(A) has developed and is implementing a plan for achieving compliance during the 8-year-period beginning on the date of enactment of this paragraph, including annual targets for compliance and active training and enforcement programs; and

''(B) has met the most recent target under subparagraph (A).

''(5) VALIDATION BY SECRETARY.—Not later than 90 days after a State or Indian tribe certification under paragraph (1), the Secretary shall—

''(A) determine whether the State or Indian tribe has demonstrated meeting the criteria of this subsection, including accurate measurement of compliance; and

''(B) if the determination is positive, validate the certification.

''(d) STATES OR INDIAN TRIBES THAT DO NOT ACHIEVE COMPLIANCE.—

''(1) REPORTING.—A State or Indian tribe that has not made a certification required under subsection (b) or (c) by the applicable deadline shall submit to the Secretary a report on—

''(A) the status of the State or Indian tribe with respect to meeting the requirements and submitting the certification; and

''(B) a plan for meeting the requirements and submitting the certification.

''(2) FEDERAL SUPPORT.—For any State or Indian tribe for which the Secretary has not validated a certification by a deadline under subsection (b) or (c), the lack of the certification may be a consideration for Federal support authorized under this section for code adoption and compliance activities.

''(3) LOCAL GOVERNMENT.—In any State or Indian tribe for which the Secretary has not validated a certification under subsection (b) or (c), a local government may be eligible for Federal support by meeting the certification requirements of subsections (b) and (c).

''(4) ANNUAL REPORTS BY SECRETARY.—

''(A) IN GENERAL.—The Secretary shall annually submit to Congress, and publish in the Federal Register, a report on—

''(i) the status of model building energy codes;

''(ii) the status of code adoption and compliance in the States and Indian tribes;

''(iii) implementation of this section; and

''(iv) improvements in energy savings over time as result of the targets established under section 307(b)(2).

''(B) IMPACTS.—The report shall include estimates of impacts of past action under this section, and potential impacts of further action, on—

''(i) upfront financial and construction costs, cost benefits and returns (using investment analysis), and lifetime energy use for buildings;

''(ii) resulting energy costs to individuals and businesses; and

''(iii) resulting overall annual building ownership and operating costs.

''(e) TECHNICAL ASSISTANCE TO STATES AND INDIAN TRIBES.—The Secretary shall provide technical assistance to States and Indian tribes to implement the goals and requirements of this section, including procedures and technical analysis for States and Indian tribes—

''(1) to improve and implement State residential and commercial building energy codes;

''(2) to demonstrate that the code provisions of the States and Indian tribes achieve equivalent or greater energy savings than the model building energy codes and targets;

''(3) to document the rate of compliance with a building energy code; and

''(4) to otherwise promote the design and construction of energy efficient buildings.

''(f) AVAILABILITY OF INCENTIVE FUNDING.—

''(1) IN GENERAL.—The Secretary shall provide incentive funding to States and Indian tribes—

''(A) to implement the requirements of this section;

''(B) to improve and implement residential and commercial building energy codes, including increasing and verifying compliance with the codes and training of State, tribal, and local building code officials to implement and enforce the codes; and

''(C) to promote building energy efficiency through the use of the codes.

''(2) ADDITIONAL FUNDING.—Additional funding shall be provided under this subsection for implementation of a plan to achieve and document full compliance with residential and commercial building energy codes under subsection (c)—

''(A) to a State or Indian tribe for which the Secretary has validated a certification under subsection (b) or (c); and

''(B) in a State or Indian tribe that is not eligible under subparagraph (A), to a local government that is eligible under this section.

''(3) TRAINING.—Of the amounts made available under this subsection, the State may use amounts required, but not to exceed $750,000 for a State, to train State and local building code officials to implement and enforce codes described in paragraph (2).

''(4) LOCAL GOVERNMENTS.—States may share grants under this subsection with local governments that implement and enforce the codes.

''(g) STRETCH CODES AND ADVANCED STANDARDS.—

''(1) IN GENERAL.—The Secretary shall provide technical and financial support for the development of stretch codes and advanced standards for residential and commercial buildings for use as—

''(A) an option for adoption as a building energy code by local, tribal, or State governments; and

''(B) guidelines for energy-efficient building design.

''(2) TARGETS.—The stretch codes and advanced standards shall be designed—

''(A) to achieve substantial energy savings compared to the model building energy codes; and

''(B) to meet targets under section 307(b), if available, at least 3 to 6 years in advance of the target years.

''(h) STUDIES.—The Secretary, in consultation with building science experts from the National Laboratories and institutions of higher education, designers and builders of energy-efficient residential and commercial buildings, code officials, and other stakeholders, shall undertake a study of the feasibility, impact, economics, and merit of—

''(1) code improvements that would require that buildings be designed, sited, and constructed in a manner that makes the buildings more adaptable in the future to become zero-net-energy after initial construction, as advances are achieved in energy-saving technologies;

''(2) code procedures to incorporate measured lifetimes, not just first-year energy use, in trade-offs and performance calculations; and

''(3) legislative options for increasing energy savings from building energy codes, including additional incentives for effective State and local action, and verification of compliance with and enforcement of a code other than by a State or local government.

''(i) EFFECT ON OTHER LAWS.—Nothing in this section or section 307 supersedes or modifies the application of sections 321 through 346 of the Energy Policy and Conservation Act (42 U.S.C. 6291 et seq.).

''(j) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section and section 307 $200,000,000, to remain available until expended.''.

(c) FEDERAL BUILDING ENERGY EFFICIENCY STANDARDS.—Section 305 of the Energy Conservation and Production Act (42 U.S.C. 6834) is amended by striking ''voluntary building energy code'' each place it appears in subsections (a)(2)(B) and (b) and inserting ''model building energy code''.

(d) MODEL BUILDING ENERGY CODES.—Section 307 of the Energy Conservation and Production Act (42 U.S.C. 6836) is amended to read as follows:

''SEC. 307. SUPPORT FOR MODEL BUILDING ENERGY CODES.

''(a) IN GENERAL.—The Secretary shall support the updating of model building energy codes.

''(b) TARGETS.—

''(1) IN GENERAL.—The Secretary shall support the updating of the model building energy codes to enable the achievement of aggregate energy savings targets established under paragraph (2).

''(2) TARGETS.—

''(A) IN GENERAL.—The Secretary shall work with State, Indian tribes, local governments, nationally recognized code and standards developers, and other interested parties to support the updating of model building energy codes by establishing 1 or more aggregate energy savings targets to achieve the purposes of this section.

''(B) SEPARATE TARGETS.—The Secretary may establish separate targets for commercial and residential buildings.

''(C) BASELINES.—The baseline for updating model building energy codes shall be the 2009 IECC for residential buildings and ASHRAE Standard 90.1–2010 for commercial buildings.

''(D) SPECIFIC YEARS.—

''(i) IN GENERAL.—Targets for specific years shall be established and revised by the Secretary through rulemaking and coordinated with nationally recognized code and standards developers at a level that—

''(I) is at the maximum level of energy efficiency that is technologically feasible and life-cycle cost effective, while accounting for the economic considerations under paragraph (4);

''(II) is higher than the preceding target; and

''(III) promotes the achievement of commercial and residential high-performance buildings through high performance energy efficiency (within the meaning of section 401 of the Energy Independence and Security Act of 2007 (42 U.S.C. 17061)).

''(ii) INITIAL TARGETS.—Not later than 1 year after the date of enactment of this clause, the Secretary shall establish initial targets under this subparagraph.

''(iii) DIFFERENT TARGET YEARS.—Subject to clause (i), prior to the applicable year, the Secretary may set a later target year for any of the model building energy codes described in subparagraph (A) if the Secretary determines that a target cannot be met.

''(iv) SMALL BUSINESS.—When establishing targets under this paragraph through rulemaking, the Secretary shall ensure compliance with the Small Business Regulatory Enforcement Fairness Act of 1996 (5 U.S.C. 601 note; Public Law 104–121).

''(3) APPLIANCE STANDARDS AND OTHER FACTORS AFFECTING BUILDING ENERGY USE.—In establishing building code targets under paragraph (2), the Secretary shall develop and adjust the targets in recognition of potential savings and costs relating to—

''(A) efficiency gains made in appliances, lighting, windows, insulation, and building envelope sealing;

''(B) advancement of distributed generation and on-site renewable power generation technologies;

''(C) equipment improvements for heating, cooling, and ventilation systems;

''(D) building management systems and SmartGrid technologies to reduce energy use; and

''(E) other technologies, practices, and building systems that the Secretary considers appropriate regarding building plug load and other energy uses.

''(4) ECONOMIC CONSIDERATIONS.—In establishing and revising building code targets under paragraph (2), the Secretary shall consider the economic feasibility of achieving the proposed targets established under this section and the potential costs and savings for consumers and building owners, including a return on investment analysis.

''(c) TECHNICAL ASSISTANCE TO MODEL BUILDING ENERGY CODE-SETTING AND STANDARD DEVELOPMENT ORGANIZATIONS.—

''(1) IN GENERAL.—The Secretary shall, on a timely basis, provide technical assistance to model building energy code-setting and standard development organizations consistent with the goals of this section.

''(2) ASSISTANCE.—The assistance shall include, as requested by the organizations, technical assistance in—

''(A) evaluating code or standards proposals or revisions;

''(B) building energy analysis and design tools;

''(C) building demonstrations;

''(D) developing definitions of energy use intensity and building types for use in model building energy codes to evaluate the efficiency impacts of the model building energy codes;

''(E) performance-based standards;

''(F) evaluating economic considerations under subsection (b)(4); and

''(G) developing model building energy codes by Indian tribes in accordance with tribal law.

''(3) AMENDMENT PROPOSALS.—The Secretary may submit timely model building energy code amendment proposals to the

model building energy code-setting and standard development organizations, with supporting evidence, sufficient to enable the model building energy codes to meet the targets established under subsection (b)(2).

''(4) ANALYSIS METHODOLOGY.—The Secretary shall make publicly available the entire calculation methodology (including input assumptions and data) used by the Secretary to estimate the energy savings of code or standard proposals and revisions.

''(d) DETERMINATION.—

''(1) REVISION OF MODEL BUILDING ENERGY CODES.—If the provisions of the IECC or ASHRAE Standard 90.1 regarding building energy use are revised, the Secretary shall make a preliminary determination not later than 90 days after the date of the revision, and a final determination not later than 15 months after the date of the revision, on whether or not the revision will—

''(A) improve energy efficiency in buildings compared to the existing model building energy code; and

''(B) meet the applicable targets under subsection (b)(2).

''(2) CODES OR STANDARDS NOT MEETING TARGETS.—

''(A) IN GENERAL.—If the Secretary makes a preliminary determination under paragraph (1)(B) that a code or standard does not meet the targets established under subsection (b)(2), the Secretary may at the same time provide the model building energy code or standard developer with proposed changes that would result in a model building energy code that meets the targets and with supporting evidence, taking into consideration—

''(i) whether the modified code is technically feasible and life-cycle cost effective;

''(ii) available appliances, technologies, materials, and construction practices; and

''(iii) the economic considerations under subsection (b)(4).

''(B) INCORPORATION OF CHANGES.—

''(i) IN GENERAL.—On receipt of the proposed changes, the model building energy code or standard developer shall have an additional 270 days to accept or reject the proposed changes of the Secretary to the model building energy code or standard for the Secretary to make a final determination.

''(ii) FINAL DETERMINATION.—A final determination under paragraph (1) shall be on the modified model building energy code or standard.

''(e) ADMINISTRATION.—In carrying out this section, the Secretary shall—

''(1) publish notice of targets and supporting analysis and determinations under this section in the Federal Register to provide an explanation of and the basis for such actions, including any supporting modeling, data, assumptions, protocols, and cost-benefit analysis, including return on investment; and

''(2) provide an opportunity for public comment on targets and supporting analysis and determinations under this section.

''(f) VOLUNTARY CODES AND STANDARDS.—Nothwithstanding any other provision of this section, any model building code or standard established under this section shall not be binding on a State, local government, or Indian tribe as a matter of Federal law.''.

PART II—WORKER TRAINING AND CAPACITY BUILDING

SEC. 821. BUILDING TRAINING AND ASSESSMENT CENTERS.

(a) IN GENERAL.—The Secretary of Energy shall provide grants to institutions of higher education (as defined in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001)) and Tribal Colleges or Universities (as defined in section 316(b) of that Act (20 U.S.C. 1059c(b)) to establish building training and assessment centers—

(1) to identify opportunities for optimizing energy efficiency and environmental performance in buildings;

(2) to promote the application of emerging concepts and technologies in commercial and institutional buildings;

(3) to train engineers, architects, building scientists, building energy permitting and enforcement officials, and building technicians in energy-efficient design and operation;

(4) to assist institutions of higher education and Tribal Colleges or Universities in training building technicians;

(5) to promote research and development for the use of alternative energy sources and distributed generation to supply heat and power for buildings, particularly energy-intensive buildings; and

(6) to coordinate with and assist State-accredited technical training centers, community colleges, Tribal Colleges or Universities, and local offices of the National Institute of Food and Agriculture and ensure appropriate services are provided under this section to each region of the United States.

(b) COORDINATION AND NONDUPLICATION.—

(1) IN GENERAL.—The Secretary shall coordinate the program with the Industrial Assessment Centers program and with other Federal programs to avoid duplication of effort.

(2) COLLOCATION.—To the maximum extent practicable, building, training, and assessment centers established under this section shall be collocated with Industrial Assessment Centers.

Subtitle B—Building Efficiency Finance

SEC. 831. LOAN PROGRAM FOR ENERGY EFFICIENCY UPGRADES TO EXISTING BUILDINGS.

Title XVII of the Energy Policy Act of 2005 (42 U.S.C. 16511 et seq.) is amended by adding at the end the following:

''SEC. 1706. BUILDING RETROFIT FINANCING PROGRAM.

''(a) DEFINITIONS.—In this section:

''(1) CREDIT SUPPORT.—The term 'credit support' means a guarantee or commitment to issue a guarantee or other forms of credit enhancement to ameliorate risks for efficiency obligations.

''(2) EFFICIENCY OBLIGATION.—The term 'efficiency obligation' means a debt or repayment obligation incurred in connection with financing a project, or a portfolio of such debt or payment obligations.

''(3) PROJECT.—The term 'project' means the installation and implementation of efficiency, advanced metering, distributed generation, or renewable energy technologies and measures in a building (or in multiple buildings on a given property) that are expected to increase the energy efficiency of the building (including fixtures) in accordance with criteria established by the Secretary.

''(b) ELIGIBLE PROJECTS.—

''(1) IN GENERAL.—Notwithstanding sections 1703 and 1705, the Secretary may provide credit support under this section, in accordance with section 1702.

''(2) INCLUSIONS.—Buildings eligible for credit support under this section include commercial, multifamily residential, industrial, municipal, government, institution of higher education, school, and hospital facilities that satisfy criteria established by the Secretary.

''(c) GUIDELINES.—

''(1) IN GENERAL.—Not later than 180 days after the date of enactment of this section, the Secretary shall—

''(A) establish guidelines for credit support provided under this section; and

''(B) publish the guidelines in the Federal Register; and

''(C) provide for an opportunity for public comment on the guidelines.

''(2) REQUIREMENTS.—The guidelines established by the Secretary under this subsection shall include—

''(A) standards for assessing the energy savings that could reasonably be expected to result from a project;

''(B) examples of financing mechanisms (and portfolios of such financing mechanisms) that qualify as efficiency obligations;

''(C) the threshold levels of energy savings that a project, at the time of issuance of credit support, shall be reasonably expected to achieve to be eligible for credit support;

''(D) the eligibility criteria the Secretary determines to be necessary for making credit support available under this section; and

''(E) notwithstanding subsections (d)(3) and (g)(2)(B) of section 1702, any lien priority requirements that the Secretary determines to be necessary, in consultation with the Director of the Office of Management and Budget, which may include—

''(i) requirements to preserve priority lien status of secured lenders and creditors in buildings eligible for credit support;

''(ii) remedies available to the Secretary under chapter 176 of title 28, United States Code, in the event of default on the efficiency obligation by the borrower; and

''(iii) measures to limit the exposure of the Secretary to financial risk in the event of default, such as—

''(I) the collection of a credit subsidy fee from the borrower as a loan loss reserve, taking into account the limitation on credit support under subsection (d);

''(II) minimum debt-to-income levels of the borrower;

''(III) minimum levels of value relative to outstanding mortgage or other debt on a building eligible for credit support;

''(IV) allowable thresholds for the percent of the efficiency obligation relative to the amount of any mortgage or other debt on an eligible building;

''(V) analysis of historic and anticipated occupancy levels and rental income of an eligible building;

''(VI) requirements of third-party contractors to guarantee energy savings that will result from a retrofit project, and whether financing on the efficiency obligation will amortize from the energy savings;

''(VII) requirements that the retrofit project incorporate protocols to measure and verify energy savings; and

''(VIII) recovery of payments equally by the Secretary and the retrofit.

''(3) EFFICIENCY OBLIGATIONS.—The financing mechanisms qualified by the Secretary under paragraph (2)(B) may include—

''(A) loans, including loans made by the Federal Financing Bank;

''(B) power purchase agreements, including energy efficiency power purchase agreements;

''(C) energy services agreements, including energy performance contracts;

''(D) property assessed clean energy bonds and other tax assessment-based financing mechanisms;

''(E) aggregate on-meter agreements that finance retrofit projects; and

''(F) any other efficiency obligations the Secretary determines to be appropriate.

''(4) PRIORITIES.—In carrying out this section, the Secretary shall prioritize—

''(A) the maximization of energy savings with the available credit support funding;

''(B) the establishment of a clear application and approval process that allows private building owners, lenders, and investors to reasonably expect to receive credit support for projects that conform to guidelines;

''(C) the distribution of projects receiving credit support under this section across

States or geographical regions of the United States; and

''(D) projects designed to achieve whole-building retrofits.

''(d) LIMITATION.—Notwithstanding section 1702(c), the Secretary shall not issue credit support under this section in an amount that exceeds—

''(1) 90 percent of the principal amount of the efficiency obligation that is the subject of the credit support; or

''(2) $10,000,000 for any single project.

''(e) AGGREGATION OF PROJECTS.—To the extent provided in the guidelines developed in accordance with subsection (c), the Secretary may issue credit support on a portfolio, or pool of projects, that are not required to be geographically contiguous, if each efficiency obligation in the pool fulfills the requirements described in this section.

''(f) APPLICATION.—

''(1) IN GENERAL.—To be eligible to receive credit support under this section, the applicant shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary determines to be necessary.

''(2) CONTENTS.—An application submitted under this section shall include assurances by the applicant that—

''(A) each contractor carrying out the project meets minimum experience level criteria, including local retrofit experience, as determined by the Secretary;

''(B) the project is reasonably expected to achieve energy savings, as set forth in the application using any methodology that meets the standards described in the program guidelines;

''(C) the project meets any technical criteria described in the program guidelines;

''(D) the recipient of the credit support and the parties to the efficiency obligation will provide the Secretary with—

''(i) any information the Secretary requests to assess the energy savings that result from the project, including historical energy usage data, a simulation-based benchmark, and detailed descriptions of the building work, as described in the program guidelines; and

''(ii) permission to access information relating to building operations and usage for the period described in the program guidelines; and

''(E) any other assurances that the Secretary determines to be necessary.

''(3) DETERMINATION.—Not later than 90 days after receiving an application, the Secretary shall make a final determination on the application, which may include requests for additional information.

''(g) FEES.—

''(1) IN GENERAL.—In addition to the fees required by section 1702(h)(1), the Secretary may charge reasonable fees for credit support provided under this section.

''(2) AVAILABILITY.—Fees collected under this section shall be subject to section 1702(h)(2).

''(h) UNDERWRITING.—The Secretary may delegate the underwriting activities under this section to 1 or more entities that the Secretary determines to be qualified.

''(i) REPORT.—Not later than 1 year after commencement of the program, the Secretary shall submit to the appropriate committees of Congress a report that describes in reasonable detail—

''(1) the manner in which this section is being carried out;

''(2) the number and type of projects supported;

''(3) the types of funding mechanisms used to provide credit support to projects;

''(4) the energy savings expected to result from projects supported by this section;

''(5) any tracking efforts the Secretary is using to calculate the actual energy savings produced by the projects; and

''(6) any plans to improve the tracking efforts described in paragraph (5).

''(j) FUNDING.—

''(1) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Secretary to carry out this section $400,000,000 for the period of fiscal years 2012 through 2021, to remain available until expended.

''(2) ADMINISTRATIVE COSTS.—Not more than 1 percent of any amounts made available to the Secretary under paragraph (1) may be used by the Secretary for administrative costs incurred in carrying out this section.''.

Subtitle C—Industrial Efficiency and Competitiveness

PART I—MANUFACTURING ENERGY EFFICIENCY

SEC. 841. STATE PARTNERSHIP INDUSTRIAL ENERGY EFFICIENCY REVOLVING LOAN PROGRAM.

Section 399A of the Energy Policy and Conservation Act (42 U.S.C. 6371h–1) is amended—

(1) in the section heading, by inserting ''**AND INDUSTRY**'' before the period at the end;

(2) by redesignating subsections (h) and (i) as subsections (i) and (j), respectively; and

(3) by inserting after subsection (g) the following:

''(h) STATE PARTNERSHIP INDUSTRIAL ENERGY EFFICIENCY REVOLVING LOAN PROGRAM.—

''(1) IN GENERAL.—The Secretary shall carry out a program under which the Secretary shall provide grants to eligible lenders to pay the Federal share of creating a revolving loan program under which loans are provided to commercial and industrial manufacturers to implement commercially available technologies or processes that significantly—

''(A) reduce systems energy intensity, including the use of energy-intensive feedstocks; and

''(B) improve the industrial competitiveness of the United States.

''(2) ELIGIBLE LENDERS.—To be eligible to receive cost-matched Federal funds under this subsection, a lender shall—

''(A) be a community and economic development lender that the Secretary certifies meets the requirements of this subsection;

''(B) lead a partnership that includes participation by, at a minimum—

''(i) a State government agency; and

''(ii) a private financial institution or other provider of loan capital;

''(C) submit an application to the Secretary, and receive the approval of the Secretary, for cost-matched Federal funds to carry out a loan program described in paragraph (1); and

''(D) ensure that non-Federal funds are provided to match, on at least a dollar-for-dollar basis, the amount of Federal funds that are provided to carry out a revolving loan program described in paragraph (1).

''(3) AWARD.—The amount of cost-matched Federal funds provided to an eligible lender shall not exceed $100,000,000 for any fiscal year.

''(4) RECAPTURE OF AWARDS.—

''(A) IN GENERAL.—An eligible lender that receives an award under paragraph (1) shall be required to repay to the Secretary an amount of cost-match Federal funds, as determined by the Secretary under subparagraph (B), if the eligible lender is unable or unwilling to operate a program described in this subsection for a period of not less than 10 years beginning on the date on which the eligible lender first receives funds made available through the award.

''(B) DETERMINATION BY SECRETARY.—The Secretary shall determine the amount of cost-match Federal funds that an eligible lender shall be required to repay to the Secretary under subparagraph (A) based on the consideration by the Secretary of—

''(i) the amount of non-Federal funds matched by the eligible lender;

''(ii) the amount of loan losses incurred by the revolving loan program described in paragraph (1); and

''(iii) any other appropriate factor, as determined by the Secretary.

''(C) USE OF RECAPTURED COST-MATCH FEDERAL FUNDS.—The Secretary may distribute to eligible lenders under this subsection each amount received by the Secretary under this paragraph.

''(5) ELIGIBLE PROJECTS.—A program for which cost-matched Federal funds are provided under this subsection shall be designed to accelerate the implementation of industrial and commercial applications of technologies or processes (including distributed generation, applications or technologies that use sensors, meters, software, and information networks, controls, and drives or that have been installed pursuant to an energy savings performance contract, project, or strategy) that—

''(A) improve energy efficiency, including improvements in efficiency and use of water, power factor, or load management;

''(B) enhance the industrial competitiveness of the United States; and

''(C) achieve such other goals as the Secretary determines to be appropriate.

''(6) EVALUATION.—The Secretary shall evaluate applications for cost-matched Federal funds under this subsection on the basis of—

''(A) the description of the program to be carried out with the cost-matched Federal funds;

''(B) the commitment to provide non-Federal funds in accordance with paragraph (2)(D);

''(C) program sustainability over a 10-year period;

''(D) the capability of the applicant;

''(E) the quantity of energy savings or energy feedstock minimization;

''(F) the advancement of the goal under this Act of 25-percent energy avoidance;

''(G) the ability to fund energy efficient projects not later than 120 days after the date of the grant award; and

''(H) such other factors as the Secretary determines appropriate.

''(7) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this subsection, $400,000,000 for the period of fiscal years 2012 through 2021.''.

SEC. 842. COORDINATION OF RESEARCH AND DEVELOPMENT OF ENERGY EFFICIENT TECHNOLOGIES FOR INDUSTRY.

(a) IN GENERAL.—As part of the research and development activities of the Industrial Technologies Program of the Department of Energy, the Secretary shall establish, as appropriate, collaborative research and development partnerships with other programs within the Office of Energy Efficiency and Renewable Energy (including the Building Technologies Program), the Office of Electricity Delivery and Energy Reliability, and the Office of Science that—

(1) leverage the research and development expertise of those programs to promote early stage energy efficiency technology development;

(2) support the use of innovative manufacturing processes and applied research for development, demonstration, and commercialization of new technologies and processes

to improve efficiency (including improvements in efficient use of water), reduce emissions, reduce industrial waste, and improve industrial cost-competitiveness; and

(3) apply the knowledge and expertise of the Industrial Technologies Program to help achieve the program goals of the other programs.

(b) REPORTS.—Not later than 2 years after the date of enactment of this Act and biennially thereafter, the Secretary shall submit to Congress a report that describes actions taken to carry out subsection (a) and the results of those actions.

SEC. 843. REDUCING BARRIERS TO THE DEPLOYMENT OF INDUSTRIAL ENERGY EFFICIENCY.

(a) DEFINITIONS.—In this section:

(1) INDUSTRIAL ENERGY EFFICIENCY.—The term ''industrial energy efficiency'' means the energy efficiency derived from commercial technologies and measures to improve energy efficiency or to generate or transmit electric power and heat, including electric motor efficiency improvements, demand response, direct or indirect combined heat and power, and waste heat recovery.

(2) INDUSTRIAL SECTOR.—The term ''industrial sector'' means any subsector of the manufacturing sector (as defined in North American Industry Classification System codes 31-33 (as in effect on the date of enactment of this Act)) establishments of which have, or could have, thermal host facilities with electricity requirements met in whole, or in part, by onsite electricity generation, including direct and indirect combined heat and power or waste recovery.

(3) SECRETARY.—The term ''Secretary'' means the Secretary of Energy.

(b) REPORT ON THE DEPLOYMENT OF INDUSTRIAL ENERGY EFFICIENCY.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Secretary shall submit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Energy and Natural Resources of the Senate a report describing—

(A) the results of the study conducted under paragraph (2); and

(B) recommendations and guidance developed under paragraph (3).

(2) STUDY.—The Secretary, in coordination with the industrial sector, shall conduct a study of the following:

(A) The legal, regulatory, and economic barriers to the deployment of industrial energy efficiency in all electricity markets (including organized wholesale electricity markets, and regulated electricity markets), including, as applicable, the following:

(i) Transmission and distribution interconnection requirements.

(ii) Standby, back-up, and maintenance fees (including demand ratchets).

(iii) Exit fees.

(iv) Life of contract demand ratchets.

(v) Net metering.

(vi) Calculation of avoided cost rates.

(vii) Power purchase agreements.

(viii) Energy market structures.

(ix) Capacity market structures.

(x) Other barriers as may be identified by the Secretary, in coordination with the industrial sector.

(B) Examples of —

(i) successful State and Federal policies that resulted in greater use of industrial energy efficiency;

(ii) successful private initiatives that resulted in greater use of industrial energy efficiency; and

(iii) cost-effective policies used by foreign countries to foster industrial energy efficiency.

(C) The estimated economic benefits to the national economy of providing the industrial sector with Federal energy efficiency matching grants of $5,000,000,000 for 5- and 10-year periods, including benefits relating to—

(i) estimated energy and emission reductions;

(ii) direct and indirect jobs saved or created;

(iii) direct and indirect capital investment;

(iv) the gross domestic product; and

(v) trade balance impacts.

(D) The estimated energy savings available from increased use of recycled material in energy-intensive manufacturing processes.

(3) RECOMMENDATIONS AND GUIDANCE.—The Secretary, in coordination with the industrial sector, shall develop policy recommendations regarding the deployment of industrial energy efficiency, including proposed regulatory guidance to States and relevant Federal agencies to address barriers to deployment.

SEC. 844. FUTURE OF INDUSTRY PROGRAM.

(a) IN GENERAL.—Section 452 of the Energy Independence and Security Act of 2007 (42 U.S.C. 17111) is amended by striking the section heading and inserting the following: ''**FUTURE OF INDUSTRY PROGRAM**''.

(b) DEFINITION OF ENERGY SERVICE PROVIDER.—Section 452(a) of the Energy Independence and Security Act of 2007 (42 U.S.C. 17111(a)) is amended—

(1) by redesignating paragraphs (3) through (5) as paragraphs (4) through (6), respectively; and

(2) by inserting after paragraph (3):

''(5) ENERGY SERVICE PROVIDER.—The term 'energy service provider' means any private company or similar entity providing technology or services to improve energy efficiency in an energy-intensive industry.''.

(c) INDUSTRIAL RESEARCH AND ASSESSMENT CENTERS.—

(1) IN GENERAL.—Section 452(e) of the Energy Independence and Security Act of 2007 (42 U.S.C. 17111(e)) is amended—

(A) by redesignating paragraphs (1) through (5) as subparagraphs (A) through (E), respectively, and indenting appropriately;

(B) by striking ''The Secretary'' and inserting the following:

''(1) IN GENERAL.—The Secretary'';

(C) in subparagraph (A) (as redesignated by subparagraph (A)), by inserting before the semicolon at the end the following: '', including assessments of sustainable manufacturing goals and the implementation of information technology advancements for supply chain analysis, logistics, system monitoring, industrial and manufacturing processes, and other purposes''; and

(D) by adding at the end the following:

''(2) CENTERS OF EXCELLENCE.—

''(A) IN GENERAL.—The Secretary shall establish a Center of Excellence at up to 10 of the highest performing industrial research and assessment centers, as determined by the Secretary.

''(B) DUTIES.—A Center of Excellence shall coordinate with and advise the industrial research and assessment centers located in the region of the Center of Excellence.

''(C) FUNDING.—Subject to the availability of appropriations, of the funds made available under subsection (f), the Secretary shall use to support each Center of Excellence not less than $500,000 for fiscal year 2012 and each fiscal year thereafter, as determined by the Secretary.

''(3) EXPANSION OF CENTERS.—The Secretary shall provide funding to establish additional industrial research and assessment centers at institutions of higher education that do not have industrial research and assessment centers established under paragraph (1), taking into account the size of, and potential energy efficiency savings for, the manufacturing base within the region of the proposed center.

''(4) COORDINATION.—

''(A) IN GENERAL.—To increase the value and capabilities of the industrial research and assessment centers, the centers shall—

''(i) coordinate with Manufacturing Extension Partnership Centers of the National Institute of Standards and Technology;

''(ii) coordinate with the Building Technologies Program of the Department of Energy to provide building assessment services to manufacturers;

''(iii) increase partnerships with the National Laboratories of the Department of Energy to leverage the expertise and technologies of the National Laboratories for national industrial and manufacturing needs;

''(iv) increase partnerships with energy service providers and technology providers to leverage private sector expertise and accelerate deployment of new and existing technologies and processes for energy efficiency, power factor, and load management;

''(v) identify opportunities for reducing greenhouse gas emissions; and

''(vi) promote sustainable manufacturing practices for small- and medium-sized manufacturers.

''(5) OUTREACH.—The Secretary shall provide funding for—

''(A) outreach activities by the industrial research and assessment centers to inform small- and medium-sized manufacturers of the information, technologies, and services available; and

''(B) a full-time equivalent employee at each center of excellence whose primary mission shall be to coordinate and leverage the efforts of the center with—

''(i) Federal and State efforts;

''(ii) the efforts of utilities and energy service providers;

''(iii) the efforts of regional energy efficiency organizations; and

''(iv) the efforts of other centers in the region of the center of excellence.

''(6) WORKFORCE TRAINING.—

''(A) IN GENERAL.—The Secretary shall pay the Federal share of associated internship programs under which students work with or for industries, manufacturers, and energy service providers to implement the recommendations of industrial research and assessment centers.

''(B) FEDERAL SHARE.—The Federal share of the cost of carrying out internship programs described in subparagraph (A) shall be 50 percent.

''(C) FUNDING.—Subject to the availability of appropriations, of the funds made available under subsection (f), the Secretary shall use to carry out this paragraph not less than $5,000,000 for fiscal year 2012 and each fiscal year thereafter.

''(7) SMALL BUSINESS LOANS.—The Administrator of the Small Business Administration shall, to the maximum practicable, expedite consideration of applications from eligible small business concerns for loans under the Small Business Act (15 U.S.C. 631 et seq.) to implement recommendations of industrial research and assessment centers established under paragraph (1).''.

SEC. 845. SUSTAINABLE MANUFACTURING INITIATIVE.

(a) IN GENERAL.—Part E of title III of the Energy Policy and Conservation Act (42 U.S.C. 6341) is amended by adding at the end the following:

''SEC. 376. SUSTAINABLE MANUFACTURING INITIATIVE.

''(a) IN GENERAL.—As part of the Industrial Technologies Program of the Department of Energy, the Secretary shall carry out a sustainable manufacturing initiative under which the Secretary, on the request of a manufacturer, shall conduct onsite technical assessments to identify opportunities for—

''(1) maximizing the energy efficiency of industrial processes and cross-cutting systems;

''(2) preventing pollution and minimizing waste;

''(3) improving efficient use of water in manufacturing processes;

''(4) conserving natural resources; and

''(5) achieving such other goals as the Secretary determines to be appropriate.

''(b) COORDINATION.—The Secretary shall carry out the initiative in coordination with the private sector and appropriate agencies, including the National Institute of Standards and Technology to accelerate adoption of new and existing technologies or processes that improve energy efficiency.

''(c) RESEARCH AND DEVELOPMENT PROGRAM FOR SUSTAINABLE MANUFACTURING AND INDUSTRIAL TECHNOLOGIES AND PROCESSES.—As part of the Industrial Technologies Program of the Department of Energy, the Secretary shall carry out a joint industry-government partnership program to research, develop, and demonstrate new sustainable manufacturing and industrial technologies and processes that maximize the energy efficiency of industrial systems, reduce pollution, and conserve natural resources.

''(d) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be to carry out this section $10,000,000 for the period of fiscal years 2012 through 2021.''.

(b) TABLE OF CONTENTS.—The table of contents of the Energy Policy and Conservation Act (42 U.S.C. prec. 6201) is amended by adding at the end of the items relating to part E of title III the following:

''Sec. 376. Sustainable manufacturing initiative.''.

SEC. 846. STUDY OF ADVANCED ENERGY TECHNOLOGY MANUFACTURING CAPABILITIES IN THE UNITED STATES.

(a) IN GENERAL.—Not later than 60 days after the date of enactment of this Act, the Secretary shall enter into an arrangement with the National Academy of Sciences under which the Academy shall conduct a study of the development of advanced manufacturing capabilities for various energy technologies, including—

(1) an assessment of the manufacturing supply chains of established and emerging industries;

(2) an analysis of—

(A) the manner in which supply chains have changed over the 25-year period ending on the date of enactment of this Act;

(B) current trends in supply chains; and

(C) the energy intensity of each part of the supply chain and opportunities for improvement;

(3) for each technology or manufacturing sector, an analysis of which sections of the supply chain are critical for the United States to retain or develop to be competitive in the manufacturing of the technology;

(4) an assessment of which emerging energy technologies the United States should focus on to create or enhance manufacturing capabilities; and

(5) recommendations on leveraging the expertise of energy efficiency and renewable energy user facilities so that best materials and manufacturing practices are designed and implemented.

(b) REPORT.—Not later than 2 years after the date on which the Secretary enters into the agreement with the Academy described in subsection (a), the Academy shall submit to the Committee on Energy and Natural Resources of the Senate, the Committee on Energy and Commerce of the House of Representatives, and the Secretary a report describing the results of the study required under this section, including any findings and recommendations.

SEC. 847. INDUSTRIAL TECHNOLOGIES STEERING COMMITTEE.

The Secretary shall establish an advisory steering committee that includes national trade associations representing energy-intensive industries or energy service providers to provide recommendations to the Secretary on planning and implementation of the Industrial Technologies Program of the Department of Energy.

PART II—SUPPLY STAR

SEC. 851. SUPPLY STAR.

Part B of title III of the Energy Policy and Conservation Act (42 U.S.C. 6291) is amended by inserting after section 324A (42 U.S.C. 6294a) the following:

''SEC. 324B. SUPPLY STAR PROGRAM.

''(a) IN GENERAL.—There is established within the Department of Energy a Supply Star program to identify and promote practices, recognize companies, and, as appropriate, recognize products that use highly efficient supply chains in a manner that conserves energy, water, and other resources.

''(b) COORDINATION.—In carrying out the program described in subsection (a), the Secretary shall—

''(1) consult with other appropriate agencies; and

''(2) coordinate efforts with the Energy Star program established under section 324A.

''(c) DUTIES.—In carrying out the Supply Star program described in subsection (a), the Secretary shall—

''(1) promote practices, recognize companies, and, as appropriate, recognize products that comply with the Supply Star program as the preferred practices, companies, and products in the marketplace for maximizing supply chain efficiency;

''(2) work to enhance industry and public awareness of the Supply Star program;

''(3) collect and disseminate data on supply chain energy resource consumption;

''(4) develop and disseminate metrics, processes, and analytical tools (including software) for evaluating supply chain energy resource use;

''(5) develop guidance at the sector level for improving supply chain efficiency;

''(6) work with domestic and international organizations to harmonize approaches to analyzing supply chain efficiency, including the development of a consistent set of tools, templates, calculators, and databases; and

''(7) work with industry, including small businesses, to improve supply chain efficiency through activities that include—

''(A) developing and sharing best practices; and

''(B) providing opportunities to benchmark supply chain efficiency.

''(d) EVALUATION.—In any evaluation of supply chain efficiency carried out by the Secretary with respect to a specific product, the Secretary shall consider energy consumption and resource use throughout the entire lifecycle of a product, including production, transport, packaging, use, and disposal.

''(e) GRANTS AND INCENTIVES.—

''(1) IN GENERAL.—The Secretary may award grants or other forms of incentives on a competitive basis to eligible entities, as determined by the Secretary, for the purposes of—

''(A) studying supply chain energy resource efficiency; and

''(B) demonstrating and achieving reductions in the energy resource consumption of commercial products through changes and improvements to the production supply and distribution chain of the products.

''(2) USE OF INFORMATION.—Any information or data generated as a result of the grants or incentives described in paragraph (1) shall be used to inform the development of the Supply Star Program.

''(f) TRAINING.—The Secretary shall use funds to support professional training programs to develop and communicate methods, practices, and tools for improving supply chain efficiency.

''(g) EFFECT OF IMPACT ON CLIMATE CHANGE.—For purposes of this section, the impact on climate change shall not be a factor in determining supply chain efficiency.

''(h) EFFECT OF OUTSOURCING OF AMERICAN JOBS.—For purposes of this section, the outsourcing of American jobs in the production of a product shall not count as a positive factor in determining supply chain efficiency.

''(i) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section $10,000,000 for the period of fiscal years 2012 through 2021.''.

PART III—ELECTRIC MOTOR REBATE PROGRAM

SEC. 861. ENERGY SAVING MOTOR CONTROL REBATE PROGRAM.

(a) ESTABLISHMENT.—Not later than January 1, 2012, the Secretary of Energy (referred to in this section as the ''Secretary'') shall establish a program to provide rebates for expenditures made by entities for the purchase and installation of a new constant speed electric motor control that reduces motor energy use by not less than 5 percent.

(b) REQUIREMENTS.—

(1) APPLICATION.—To be eligible to receive a rebate under this section, an entity shall submit to the Secretary an application in such form, at such time, and containing such information as the Secretary may require, including—

(A) demonstrated evidence that the entity purchased a constant speed electric motor control that reduces motor energy use by not less than 5 percent; and

(B) the physical nameplate of the installed motor of the entity to which the energy saving motor control is attached.

(2) AUTHORIZED AMOUNT OF REBATE.—The Secretary may provide to an entity that meets the requirements of paragraph (1) a rebate the amount of which shall be equal to the product obtained by multiplying—

(A) the nameplate horsepower of the electric motor to which the energy saving motor control is attached; and

(B) $25.

(c) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this section $5,000,000 for each of fiscal years 2012 and 2013, to remain available until expended.

PART IV—TRANSFORMER REBATE PROGRAM

SEC. 871. ENERGY EFFICIENT TRANSFORMER REBATE PROGRAM.

(a) DEFINITION OF QUALIFIED TRANSFORMER.—In this section, the term ''qualified transformer'' means a transformer that meets or exceeds the National Electrical Manufacturers Association (NEMA) Premium Efficiency designation, calculated to 2 decimal points, as having 30 percent fewer losses than the NEMA TP-1-2002 efficiency standard for a transformer of the same number of phases and capacity, as measured in kilovolt-amperes.

(b) ESTABLISHMENT.—Not later than January 1, 2012, the Secretary of Energy (referred to in this section as the ''Secretary'') shall establish a program to provide rebates for expenditures made by owners of commercial buildings and multifamily residential buildings for the purchase and installation of a new energy efficient transformers.

(c) REQUIREMENTS.—

(1) APPLICATION.—To be eligible to receive a rebate under this section, an owner shall submit to the Secretary an application in such form, at such time, and containing such information as the Secretary may require,

including demonstrated evidence that the owner purchased a qualified transformer.

(2) AUTHORIZED AMOUNT OF REBATE.—For qualified transformers, rebates, in dollars per kilovolt-ampere (referred to in this paragraph as ''kVA'') shall be—

(A) for 3-phase transformers—

(i) with a capacity of not greater than 10 kVA, $15;

(ii) with a capacity of not less than 10 kVA and not greater than 100 kVA, the difference between 15 and the quotient obtained by dividing—

(I) the difference between—

(aa) the capacity of the transformer in kVA; and

(bb) 10; by

(II) 9; and

(iii) with a capacity greater than or equal to 100 kVA, $5; and

(B) for single-phase transformers, 75 percent of the rebate for a 3-phase transformer of the same capacity.

(d) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this section $5,000,000 for each of fiscal years 2012 and 2013, to remain available until expended.

Subtitle D—Federal Agency Energy Efficiency

SEC. 881. ADOPTION OF PERSONAL COMPUTER POWER SAVINGS TECHNIQUES BY FEDERAL AGENCIES.

(a) IN GENERAL.—Not later than 360 days after the date of enactment of this Act, the Secretary of Energy, in consultation with the Secretary of Defense, the Secretary of Veterans Affairs, and the Administrator of General Services, shall issue guidance for Federal agencies to employ advanced tools allowing energy savings through the use of computer hardware, energy efficiency software, and power management tools.

(b) REPORTS ON PLANS AND SAVINGS.—Not later than 180 days after the date of the issuance of the guidance under subsection (a), each Federal agency shall submit to the Secretary of Energy a report that describes—

(1) the plan of the agency for implementing the guidance within the agency; and

(2) estimated energy and financial savings from employing the tools described in subsection (a).

SEC. 882. AVAILABILITY OF FUNDS FOR DESIGN UPDATES.

Section 3307 of title 40, United States Code, is amended—

(1) by redesignating subsections (d) through (h) as subsections (e) through (i), respectively; and

(2) by inserting after subsection (c) the following:

''(d) AVAILABILITY OF FUNDS FOR DESIGN UPDATES.—

''(1) IN GENERAL.—Subject to paragraph (2), for any project for which congressional approval is received under subsection (a) and for which the design has been substantially completed but construction has not begun, the Administrator of General Services may use appropriated funds to update the project design to meet applicable Federal building energy efficiency standards established under section 305 of the Energy Conservation and Production Act (42 U.S.C. 6834) and other requirements established under section 3312.

''(2) LIMITATION.—The use of funds under paragraph (1) shall not exceed 125 percent of the estimated energy or other cost savings associated with the updates as determined by a life-cycle cost analysis under section 544 of the National Energy Conservation Policy Act (42 U.S.C. 8254).''.

SEC. 883. BEST PRACTICES FOR ADVANCED METERING.

Section 543(e) of the National Energy Conservation Policy Act (42 U.S.C. 8253(e) is amended by striking paragraph (3) and inserting the following:

''(3) PLAN.—

''(A) IN GENERAL.—Not later than 180 days after the date on which guidelines are established under paragraph (2), in a report submitted by the agency under section 548(a), each agency shall submit to the Secretary a plan describing the manner in which the agency will implement the requirements of paragraph (1), including—

''(i) how the agency will designate personnel primarily responsible for achieving the requirements; and

''(ii) a demonstration by the agency, complete with documentation, of any finding that advanced meters or advanced metering devices (as those terms are used in paragraph (1)), are not practicable.

''(B) UPDATES.—Reports submitted under subparagraph (A) shall be updated annually.

''(4) BEST PRACTICES REPORT.—

''(A) IN GENERAL.—Not later than 180 days after the date of enactment of the Energy Savings and Industrial Competitiveness Act of 2012, the Secretary of Energy, in consultation with the Secretary of Defense and the Administrator of General Services, shall develop, and issue a report on, best practices for the use of advanced metering of energy use in Federal facilities, buildings, and equipment by Federal agencies.

''(B) UPDATING.—The report described under subparagraph (A) shall be updated annually.

''(C) COMPONENTS.—The report shall include, at a minimum—

''(i) summaries and analysis of the reports by agencies under paragraph (3);

''(ii) recommendations on standard requirements or guidelines for automated energy management systems, including—

''(I) potential common communications standards to allow data sharing and reporting;

''(II) means of facilitating continuous commissioning of buildings and evidence-based maintenance of buildings and building systems; and

''(III) standards for sufficient levels of security and protection against cyber threats to ensure systems cannot be controlled by unauthorized persons; and

''(iii) an analysis of—

''(I) the types of advanced metering and monitoring systems being piloted, tested, or installed in Federal buildings; and

''(II) existing techniques used within the private sector or other non-Federal government buildings.''.

SEC. 884. FEDERAL ENERGY MANAGEMENT AND DATA COLLECTION STANDARD.

Section 543 of the National Energy Conservation Policy Act (42 U.S.C. 8253) is amended—

(1) by redesignating the second subsection (f) (as added by section 434(a) of Public Law 110–140 (121 Stat. 1614)) as subsection (g); and

(2) in subsection (f)(7), by striking subparagraph (A) and inserting the following:

''(A) IN GENERAL.—For each facility that meets the criteria established by the Secretary under paragraph (2)(B), the energy manager shall use the web-based tracking system under subparagraph (B)—

''(i) to certify compliance with the requirements for—

''(I) energy and water evaluations under paragraph (3);

''(II) implementation of identified energy and water measures under paragraph (4); and

''(III) follow-up on implemented measures under paragraph (5); and

''(ii) to publish energy and water consumption data on an individual facility basis.''.

SEC. 885. ELECTRIC VEHICLE CHARGING INFRASTRUCTURE.

Section 804(4) of the National Energy Conservation Policy Act (42 U.S.C. 8287c(4)) is amended—

(1) in subparagraph (A), by striking ''or'' after the semicolon;

(2) in subparagraph (B), by striking the period at the end and inserting ''; or''; and

(3) by adding at the end the following:

''(C) a measure to support the use of electric vehicles or the fueling or charging infrastructure necessary for electric vehicles.''.

SEC. 886. FEDERAL PURCHASE REQUIREMENT.

Section 203 of the Energy Policy Act of 2005 (42 U.S.C. 15852) is amended—

(1) in subsections (a) and (b)(2), by striking ''electric energy'' each place it appears and inserting ''electric, direct, and thermal energy'';

(2) in subsection (b)(2)—

(A) by inserting '', or avoided by,'' after ''generated from''; and

(B) by inserting ''(including ground-source, reclaimed, and ground water)''after ''geothermal'';

(3) by redesignating subsection (d) as subsection (e); and

(4) by inserting after subsection (c) the following:

''(d) SEPARATE CALCULATION.—Renewable energy produced at a Federal facility, on Federal land, or on Indian land (as defined in section 2601 of the Energy Policy Act of 1992 (25 U.S.C. 3501))—

''(1) shall be calculated (on a BTU-equivalent basis) separately from renewable energy used; and

''(2) may be used individually or in combination to comply with subsection (a).''.

SEC. 887. STUDY ON FEDERAL DATA CENTER CONSOLIDATION.

(a) IN GENERAL.—The Secretary of Energy shall conduct a study on the feasibility of a government-wide data center consolidation, with an overall Federal target of a minimum of 800 Federal data center closures by October 1, 2015.

(b) COORDINATION.—In conducting the study, the Secretary shall coordinate with Federal data center program managers, facilities managers, and sustainability officers.

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the Secretary shall submit to Congress a report that describes the results of the study, including a description of agency best practices in data center consolidation.

Subtitle E—Miscellaneous

SEC. 891. OFFSETS.

(a) ZERO-NET ENERGY COMMERCIAL BUILDINGS INITIATIVE.—Section 422(f) of the Energy Independence and Security Act of 2007 (42 U.S.C. 17082(f)) is amended by striking paragraphs (2) through (4) and inserting the following:

''(2) $50,000,000 for each of fiscal years 2009 through 2012;

''(3) $100,000,000 for fiscal year 2013; and

''(4) $200,000,000 for each of fiscal years 2014 through 2018.''.

(b) ENERGY SUSTAINABILITY AND EFFICIENCY GRANTS AND LOANS FOR INSTITUTIONS.—Subsection (j) of section 399A of the Energy Policy and Conservation Act (42 U.S.C. 6371h–1) (as redesignated by section 841(2)) is amended—

(1) in paragraph (1), by striking ''through 2013'' and inserting ''and 2010, $100,000,000 for each of fiscal years 2011 and 2012, and $250,000,000 for fiscal year 2013''; and

(2) in paragraph (2), by striking ''through 2013'' and inserting ''and 2010, $100,000,000 for each of fiscal years 2011 and 2012, and $425,000,000 for fiscal year 2013''.

(c) WASTE ENERGY RECOVERY INCENTIVE PROGRAM.—Section 373(f)(1) of the Energy

Policy and Conservation Act (42 U.S.C. 6343(f)(1)) is amended—

(1) by redesignating subparagraph (B) as subparagraph (D); and

(2) by striking subparagraph (A) and inserting the following:

''(A) $100,000,000 for fiscal year 2008;

''(B) $200,000,000 for each of fiscal years 2009 and 2010;

''(C) $100,000,000 for each of fiscal years 2011 and 2012; and''.

(d) ENERGY-INTENSIVE INDUSTRIES PROGRAM.—Section 452(f)(1) of the Energy Independence and Security Act of 2007 (42 U.S.C. 17111(f)(1)) is amended—

(1) in subparagraph (D), by striking ''$202,000,000'' and inserting ''$102,000,000''; and

(2) in subparagraph (E), by striking ''$208,000,000'' and inserting ''$108,000,000''.

SEC. 892. ADVANCE APPROPRIATIONS REQUIRED.

The authorization of amounts under this title and the amendments made by this title shall be effective for any fiscal year only to the extent and in the amount provided in advance in appropriations Acts.

SA 2617. Mr. COONS (for himself, Mr. WYDEN, Mr. AKAKA, Mr. FRANKEN, Mr. UDALL of New Mexico, and Mr. SANDERS) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of title VII, add the following:

SEC. 709. SUNSET.

(a) IN GENERAL.—Except as provided in subsection (b), this title shall cease to have effect five years after the date of enactment of this Act.

(b) EXCEPTION.—With respect to any particular disclosure or sharing that occurred before the date on which the provisions referred to in subsection (a) cease to have effect, such provisions shall continue in effect.

SA 2618. Mr. AKAKA (for himself, Mr. BLUMENTHAL, Mr. COONS, Mr. FRANKEN, Mr. SANDERS, Mr. UDALL of New Mexico, and Mr. WYDEN) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 105, after the end of the matter between lines 11 and 12, insert the following:

SEC. 205. PRIVACY BREACH REQUIREMENTS.

(a) IN GENERAL.—Subchapter II of chapter 35 of title 44, United States Code, as amended by section 201 of this Act, is amended by adding at the end the following:

''§ 3559. Privacy breach requirements

''(a) POLICIES AND PROCEDURES.—The Secretary shall establish and oversee policies and procedures for agencies to follow in the event of a breach of information security involving the disclosure of personally identifiable information, including requirements for—

''(1) timely notice to the individuals whose personally identifiable information could be compromised as a result of such breach;

''(2) timely reporting to a Federal cybersecurity center (as defined in section 708 of the Cybersecurity Act of 2012), as designated by the Secretary; and

''(3) additional actions as necessary and appropriate, including data breach analysis, fraud resolution services, identity theft insurance, and credit protection or monitoring services.

''(b) REQUIRED AGENCY ACTION.—The head of each agency shall ensure that actions taken in response to a breach of information security involving the disclosure of personally identifiable information under the authority or control of the agency comply with policies and procedures established by the Secretary under subsection (a).

''(c) REPORT.—Not later than March 1 of each year, the Secretary shall report to Congress on agency compliance with the policies and procedures established under subsection (a).''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for subtitle II for chapter 35 of title 44, United States Code, as amended by section 201 of this Act, is amended by adding at the end the following: ''3559. Privacy breach requirements.''.

SEC. 206. AMENDMENTS TO THE E-GOVERNMENT ACT OF 2002.

Section 208(b)(1)(A) of the E-Government Act of 2002 (44 U.S.C. 3501 note; Public Law 107–347) is amended—

(1) in clause (i), by striking ''or'' at the end;

(2) in clause (ii), by striking the period at the end and inserting ''; or''; and

(3) by adding at the end the following:

''(iii) using information in an identifiable form purchased, or subscribed to for a fee, from a commercial data source.''.

SEC. 207. AUTHORITY OF THE DIRECTOR OF THE OFFICE OF MANAGEMENT AND BUDGET WITH RESPECT TO FEDERAL INFORMATION POLICY.

Section 3504(g) of title 44, United States Code, is amended—

(1) paragraph (1), by striking ''and'' at the end;

(2) in paragraph (2), by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following:

''(3) designate a Federal Chief Privacy Officer within the Office of Management and Budget who is a noncareer appointee in a Senior Executive Service position and who is a trained and experienced privacy professional to carry out the responsibilities of the Director with regard to privacy.''.

SEC. 208. CIVIL REMEDIES UNDER THE PRIVACY ACT.

Section 552a(g)(4)(A) of title 5, United States Code, is amended—

(1) by striking ''actual damages'' and inserting ''provable damages, including damages that are not pecuniary damages,''; and

(2) by striking '', but in no case shall a person entitled to recovery receive less than the sum of $1,000'' and inserting ''or the sum of $1,000, whichever is greater.''.

On page 188, lines 5 through 7, strike ''the Chief Privacy and Civil Liberties Officer of the Department of Justice and the Chief Privacy Officer of the Department'' and insert ''the Federal Chief Privacy Officer''.

On page 191, line 19, strike ''actual damages'' and insert ''provable damages, including damages that are not pecuniary damages,''

SA 2619. Mr. DEMINT submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. RIGHT TO WORK.

(a) AMENDMENTS TO THE NATIONAL LABOR RELATIONS ACT.—

(1) RIGHTS OF EMPLOYEES.—Section 7 of the National Labor Relations Act (29 U.S.C. 157) is amended by striking ''except to'' and all that follows through ''authorized in section 8(a)(3)''.

(2) UNFAIR LABOR PRACTICES.—Section 8 of the National Labor Relations Act (29 U.S.C. 158) is amended—

(A) in subsection (a)(3), by striking '': *Provided*, That'' and all that follows through ''retaining membership'';

(B) in subsection (b)—

(i) in paragraph (2), by striking ''or to discriminate'' and all that follows through ''retaining membership''; and

(ii) in paragraph (5), by striking ''covered by an agreement authorized under subsection (a)(3) of this section''; and

(C) in subsection (f), by striking clause (2) and redesignating clauses (3) and (4) as clauses (2) and (3), respectively.

(b) AMENDMENT TO THE RAILWAY LABOR ACT.—Section 2 of the Railway Labor Act (45 U.S.C. 152) is amended by striking paragraph Eleven.

SA 2620. Mr. HOEVEN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 109, strike line 17 and all that follows through page 110, line 20, and insert the following:

institutions and to provide funds to the military service academies to establish cybersecurity test beds capable of realistic modeling of real-time cyber attacks and defenses.

(B) REQUIREMENT.—The test beds established under subparagraph (A) shall be sufficiently large in order to model the scale and complexity of real world networks and environments.

(3) PURPOSE.—The purpose of the program established under paragraph (2) shall be to support the rapid development of new cybersecurity defenses, techniques, and processes by improving understanding and assessing the latest technologies in a real-world environment.

(e) COORDINATION WITH OTHER RESEARCH INITIATIVES.—The Director shall to the extent practicable, coordinate research and development activities under this section with other ongoing research and development security-related initiatives, including research being conducted by—

(1) the National Institute of Standards and Technology;

(2) the Department;

(3) other Federal agencies;

(4) other Federal and private research laboratories, research entities, the military service academies, and universities and institutions of higher education, and relevant nonprofit organizations; and

---

AUTHORITY FOR COMMITTEES TO MEET

COMMITTEE ON AGRICULTURE, NUTRITION, AND FORESTRY

Mr. LIEBERMAN. Mr. President, I ask unanimous consent that the Committee on Agriculture, Nutrition, and Forestry be authorized to meet during the session of the Senate on July 26, 2012, at 9:30 a.m. in room SR 328A of the Russell Senate Office Building.

The PRESIDING OFFICER. Without objection, it is so ordered.

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

Mr. LIEBERMAN. Mr. President, I ask unanimous consent that the Committee on Banking, Housing, and Urban Affairs be authorized to meet during the session of the Senate on July 26, 2012, at 10 a.m. to conduct a hearing entitled ''The Financial Stability Oversight Council Annual Report to Congress.''

The PRESIDING OFFICER. Without objection, it is so ordered.

COMMITTEE ON FOREIGN RELATIONS

Mr. LIEBERMAN. Mr. President, I ask unanimous consent that the Committee on Foreign Relations be authorized to meet during the session of the Senate on July 26, 2012, at 9:30 a.m.

The PRESIDING OFFICER. Without objection, it is so ordered.

COMMITTEE ON HEALTH, EDUCATION, LABOR, AND PENSIONS

Mr. LIEBERMAN. Mr. President, I ask unanimous consent that the Committee on Health, Education, Labor, and Pensions be authorized to meet during the session of the Senate, to conduct a hearing entitled ''CCDBG Reauthorization: Helping to Meet the Child Care Needs of American Families'' on July 26, 2012, at 10 a.m. in room 430 of the Dirksen Senate Office Building.

The PRESIDING OFFICER. Without objection, it is so ordered.

COMMITTEE ON INDIAN AFFAIRS

Mr. LIEBERMAN. Mr. President, I ask unanimous consent that the Committee on Indian Affairs be authorized to meet during the session of the Senate on July 26, 2012, in room SD–628 of the Dirksen Senate Office Building, at 2:15 p.m., to conduct a hearing entitled ''Regulation of Tribal Gaming: From Brick & Mortar to the Internet.''

The PRESIDING OFFICER. Without objection, it is so ordered.

COMMITTEE ON THE JUDICIARY

Mr. LIEBERMAN. Mr. President, I ask unanimous consent that the Committee on the Judiciary be authorized to meet during the session of the Senate, on July 26, 2012 at 10 a.m., in room SD–226 of the Dirksen Senate Office Building, to conduct an executive business meeting.

The PRESIDING OFFICER. Without objection, it is so ordered.

COMMITTEE ON THE JUDICIARY

Mr. LIEBERMAN. Mr. President, I ask unanimous consent that the Committee on the Judiciary be authorized to meet during the session of the Senate, on July 26, 2012 at 1 p.m., in room SD–226 of the Dirksen Senate Office Building, to conduct a hearing entitled ''Nominations.''

The PRESIDING OFFICER. Without objection, it is so ordered.

SELECT COMMITTEE ON INTELLIGENCE

Mr. LIEBERMAN. Mr. President, I ask unanimous consent that the Select Committee on Intelligence be authorized to meet during the session of the Senate on July 26, 2012, at 2:30 p.m.

The PRESIDING OFFICER. Without objection, it is so ordered.

PRIVILEGES OF THE FLOOR

Mr. CARDIN. Mr. President, I ask unanimous consent that Hala Furst, a Presidential Management Fellow on detail to the Homeland Security and Governmental Affairs Committee, be granted the privileges of the floor for the duration of the debate on S. 3414.

The PRESIDING OFFICER. Without objection, it is so ordered.

FOR THE RELIEF OF SOPURUCHI CHUKWUEKE

On Wednesday, July 25, 2012, the Senate passed S. 285, as amended, as follows:

S. 285

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. ADJUSTMENT OF STATUS.

(a) IN GENERAL.—Notwithstanding any other provision of law, for the purposes of the Immigration and Nationality Act (8 U.S.C. 1101 et seq.), Sopuruchi Chukwueke shall be deemed to have been lawfully admitted to, and remained in, the United States, and shall be eligible for adjustment of status to that of an alien lawfully admitted for permanent residence under section 245 of the Immigration and Nationality Act (8 U.S.C. 1255) upon filing an application for such adjustment of status.

(b) APPLICATION AND PAYMENT OF FEES.—Subsection (a) shall apply only if the application for adjustment of status is filed with appropriate fees not later than 2 years after the date of the enactment of this Act.

(c) REDUCTION OF IMMIGRANT VISA NUMBERS.—Upon the granting of permanent resident status to Sopuruchi Chukwueke, the Secretary of State shall instruct the proper officer to reduce by 1, during the current or next following fiscal year, the total number of immigrant visas that are made available to natives of the country of the birth of Sopuruchi Chukwueke under section 202(a)(2) of the Immigration and Nationality Act (8 U.S.C. 1152(a)(2)).

(d) DENIAL OF PREFERENTIAL IMMIGRATION TREATMENT FOR CERTAIN RELATIVES.—The natural parents, brothers, and sisters of Sopuruchi Victor Chukwueke shall not, by virtue of such relationship, be accorded any right, privilege, or status under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

UNANIMOUS CONSENT AGREEMENT—EXECUTIVE CALENDAR

Mr. SCHUMER. Mr. President, I ask unanimous consent that at a time to be determined by the majority leader, in consultation with the Republican leader, the Senate proceed to executive session to consider Calendar No. 518; that there be 60 minutes for debate equally divided in the usual form; that upon the use or yielding back of the time, the Senate proceed to vote, without intervening action or debate, on the nomination; that the nomination be subject to a 60-vote threshold, the motion to reconsider be considered made and laid upon the table, with no intervening action or debate; that no further motions be in order to the nomination; that any statements related to the nomination be printed in the RECORD; and that the President be immediately notified of the Senate's action and the Senate then resume legislative session.

The PRESIDING OFFICER. Without objection, it is so ordered.

EXECUTIVE SESSION

EXECUTIVE CALENDAR

Mr. SCHUMER. Mr. President, I ask unanimous consent that the Senate proceed to executive session to consider the following nominations: Calendar Nos. 839, 840, 842, 843, 844, 845, 846, 847, 848, 849, 850, 851, 852, 853, 854, 855, 856, 857, and all the nominations placed on the Secretary's desk in the Army, Air Force, and Navy; that the nominations be confirmed en bloc; the motions to reconsider be made and laid upon the table with no intervening action or debate; that no further motions be in order to any of the nominations; that any related statements be printed in the RECORD; that the President be immediately notified of the Senate's action, and the Senate then resume legislative session.

The PRESIDING OFFICER. Without objection, it is so ordered.

The nominations considered and confirmed en bloc are as follows:

IN THE AIR FORCE

The following Air National Guard of the United States officer for appointment in the Reserve of the Air Force to the grade indicated under title 10, U.S.C., sections 12203 and 12212:

To be brigadier general

Colonel Edward E. Metzgar

The following Air National Guard of the United States officer for appointment in the Reserve of the Air Force to the grade indicated under title 10, U.S.C., sections 12203 and 12212:

To be brigadier general

Colonel Russ A. Walz

The following named officer for appointment in the United States Air Force to the grade indicated under title 10, U.S.C., section 624:

To be major general

Brig. Gen. Timothy M. Ray

The following named officer for appointment in the United States Air Force to the grade indicated while assigned to a position of importance and responsibility under title 10, U.S.C., section 601:

To be general

Lt. Gen. Paul J. Selva

The following named officer for appointment as the Vice Chief of the National Guard Bureau and for appointment to the grade indicated in the Reserve of the Air Force under title 10, U.S.C., sections 10505 and 601:

To be lieutenant general

Maj. Gen. Joseph L. Lengyel

The following named officer for appointment in the United States Air Force to the grade indicated under title 10, U.S.C., section 624:

To be major general

Brig. Gen. Howard D. Stendahl

IN THE ARMY

The following named officer for appointment in the Reserve of the Army to the

grade indicated under title 10, U.S.C., section 12203:

To be major general

Brig. Gen. Lawrence w. Brock

The following Army National Guard of the United States officer for appointment in the Reserve of the Army to the grade indicated under title 10, U.S.C., section 12203 and 12211:

To be major general

Brig. Gen. Reynold N. Hoover

The following named officer for appointment in the United States Army to the grade indicated while assigned to a position of importance and responsibility under title 10, U.S.C., section 601:

To be lieutenant general

Maj. Gen. James O. Barclay, III

The following named officer for appointment in the United States Army to the grade indicated while assigned to a position of importance and responsibility under title 10, U.S.C., section 601:

To be lieutenant general

Lt. Gen. Donald M. Campbell, Jr.

The following named officer for appointment as the Chief of the National Guard Bureau and for appointment to the grade indicated in the Reserve of the Army under title 10, U.S.C., sections 10502 and 601:

To be general

Lt. Gen. Frank J. Grass

The following named officer for appointments in the United States Army to the grade indicated while assigned to a position of importance and responsibility under title 10, U.S.C., section 601:

To be lieutenant general

Maj. Gen. David R. Hogg

The following Army National Guard of the United States officer for appointment in the Reserve of the Army to the grade indicated under title 10, U.S.C., section 12203 and 12211:

To be major general

Brig. Gen. Joyce L. Stevens

IN THE NAVY

The following named officer for appointment in the United States Navy to the grade indicated while assigned to a position of importance and responsibility under title 10, U.S.C., section 601:

To be vice admiral

Vice Adm. Allen G. Myers

The following named officers for appointment in the United States Navy to the grade indicated under title 10, U.S.C., section 624:

To be rear admiral (lower half)

Captain John D. Alexander
Captain Bret C. Batchelder
Captain Ronald A. Boxall
Captain Robert P. Burke
Captain David J. Hahn
Captain Alexander L. Krongard
Captain Andrew L. Lewis
Captain Bruce H. Lindsey
Captain Dee L. Mewbourne
Captain John P. Neagley
Captain Partick A. Piercey
Captain Markham K. Rich
Captain Charles A. Richard
Captain Cynthia M. Thebaud
Captain Brad Williamson
Captain Ricky L. Williamson

The following named officer for appointment to the grade of Admiral in the United States Navy while assigned to a position of importance and responsibility under title 10, U.S.C., section 601 and title 42, U.S.C., section 7158;

To be admiral

Vice Adm. John M. Richardson

The following named officer from appointment in the United States Navy to the grade indicated while assigned to a position of importance and responsibility under title 10, U.S.C., section 601:

To be vice admiral

Rear Adm. David A. Dunaway

IN THE MARINE CORPS

The following named officer for appointment to the grade of general in the United States Marine Corps while assigned to a position of importance and responsibility under title 10, U.S.C., section 601:

To be general

Lt. Gen. John F. Kelly

NOMINATIONS PLACED ON THE SECRETARY'S DESK

IN THE AIR FORCE

PN1545 AIR FORCE nominations (89) beginning JOLENE A. AINSWORTH, and ending DAVID C. ZIMMERMAN, which nominations were received by the Senate and appeared in the Congressional Record of April 23, 2012.

PN1781 AIR FORCE nominations (2) beginning UCHENNA L. UMEH, and ending DANIEL X. CHOI, which nominations were received by the Senate and appeared in the Congressional Record of June 25, 2012.

PN1782 AIR FORCE nominations (14) beginning CATHERINE M. FAHLING, and ending LE T. ZIMMERMAN, which nominations were received by the Senate and appeared in the Congressional Record of June 25, 2012.

PN1821 AIR FORCE nominations (3) beginning SEAN J. HISLOP, and ending LUCAS P. NEFF, which nominations were received by the Senate and appeared in the Congressional Record of July 17, 2012.

IN THE ARMY

PN1785 ARMY nomination of Karen A. Baldi, which was received by the Senate and appeared in the Congressional Record of June 25, 2012.

PN1786 ARMY nomination of Christopher W. Soika, which was received by the Senate and appeared in the Congressional Record of June 25, 2012.

PN1787 ARMY nomination of Luis A. Riveraberrios, which was received by the Senate and appeared in the Congressional Record of June 25, 2012.

PN1788 ARMY nomination of Kimon A. Nicolaides, which was received by the Senate and appeared in the Congressional Record of June 25, 2012.

PN1789 ARMY nominations (2) beginning PENNY P. KALUA, and ending JOSEPH A. TRINIDAD, which nominations were received by the Senate and appeared in the Congressional Record of June 25, 2012.

PN1822 ARMY nominations (333) beginning CHAD S. ABBEY, and ending JARED K. ZOTZ, which nominations were received by the Senate and appeared in the Congressional Record of July 17, 2012.

PN1823 ARMY nominations (58) beginning JEFFREY E. AYCOCK, and ending ERIC W. YOUNG, which nominations were received by the Senate and appeared in the Congressional Record of July 17, 2012.

PN1824 ARMY nominations (8) beginning BRENT A. BECKLEY, and ending STEPHEN J. WARD, which nominations were received by the Senate and appeared in the Congressional Record of July 17, 2012.

PN1825 ARMY nomination of Brian J. Eastridge, which was received by the Senate and appeared in the Congressional Record of July 17, 2012.

IN THE NAVY

PN1809 NAVY nominations (106) beginning JOEL A. AHLGRIM, and ending MARK L. WOODBRIDGE, which nominations were received by the Senate and appeared in the Congressional Record of July 11, 2012.

PN1810 NAVY nominations (15) beginning JOHN E. BISSELL, and ending STEPHEN S. YUNE, which nominations were received by the Senate and appeared in the Congressional Record of July 11, 2012.

PN1811 NAVY nominations (37) beginning ROBERT L. ANDERSON, II, and ending CAROL B. ZWIEBACH, which nominations were received by the Senate and appeared in the Congressional Record of July 11, 2012.

PN1812 NAVY nominations (15) beginning MARC S. BREWEN, and ending DUSTIN E. WALLACE, which nominations were received by the Senate and appeared in the Congressional Record of July 11, 2012.

PN1813 NAVY nominations (87) beginning LUCELINA B. BADURA, and ending WILLIAM A. YOUNG, which nominations were received by the Senate and appeared in the Congressional Record of July 11, 2012.

PN1814 NAVY nominations (20) beginning JASON W. ADAMS, and ending SHAWN M. TRIGGS, which nominations were received by the Senate and appeared in the Congressional Record of July 11, 2012.

PN1815 NAVY nominations (20) beginning DAVID L. CLINE, and ending DAVID S. YANG, which nominations were received by the Senate and appeared in the Congressional Record of July 11, 2012.

PN1816 NAVY nominations (25) beginning EMILY Z. ALLEN, and ending JONATHAN P. WITHAM, which nominations were received by the Senate and appeared in the Congressional Record of July 11, 2012.

LEGISLATIVE SESSION

The PRESIDING OFFICER. Under the previous order, the Senate resumes legislative session.

HAQQANI NETWORK TERRORIST DESIGNATION ACT OF 2012

Mr. SCHUMER. Mr. President, I ask the Chair to lay before the Senate a message from the House with respect to S. 1959.

The Presiding officer laid before the Senate the following message from the House of Representatives:

Resolved, That the bill from the Senate (S. 1959) entitled ''An Act to require a report on the designation of the Haqqani Network as a foreign terrorist organization and for other purposes,'' do pass with the following amendment:

Strike out all after the enacting clause and insert:

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Haqqani Network Terrorist Designation Act of 2012''.

SEC. 2. REPORT ON DESIGNATION OF THE HAQQANI NETWORK AS A FOREIGN TERRORIST ORGANIZATION.

(a) FINDINGS.—Congress makes the following findings:

(1) A report of the Congressional Research Service on relations between the United States and Pakistan states that ''[t]he terrorist network led by Jalaluddin Haqqani and his son Sirajuddin, based in the FATA, is commonly identified as the most dangerous of Afghan insurgent groups battling U.S.-led forces in eastern Afghanistan''.

(2) The report further states that, in mid-2011, the Haqqanis undertook several high-visibility attacks in Afghanistan. First, a late June assault on the Intercontinental Hotel in Kabul by 8 Haqqani gunmen and suicide bombers left 18 people dead. Then, on September 10, a truck bomb attack on a United States military base by Haqqani fighters in the Wardak province injured 77 United States troops and killed 5 Afghans. A September 13 attack on the United

States Embassy compound in Kabul involved an assault that sparked a 20-hour-long gun battle and left 16 Afghans dead, 5 police officers and at least 6 children among them.

(3) The report further states that ''U.S. and Afghan officials concluded the Embassy attackers were members of the Haqqani network''.

(4) In September 22, 2011, testimony before the Committee on Armed Services of the Senate, Chairman of the Joint Chiefs of Staff Admiral Mullen stated that ''[t]he Haqqani network, for one, acts as a veritable arm of Pakistan's Inter-Services Intelligence agency. With ISI support, Haqqani operatives plan and conducted that [September 13] truck bomb attack, as well as the assault on our embassy. We also have credible evidence they were behind the June 28th attack on the Intercontinental Hotel in Kabul and a host of other smaller but effective operations''.

(5) In October 27, 2011, testimony before the Committee on Foreign Affairs of the House of Representatives, Secretary of State Hillary Clinton stated that ''we are taking action to target the Haqqani leadership on both sides of the border. We're increasing international efforts to squeeze them operationally and financially. We are already working with the Pakistanis to target those who are behind a lot of the attacks against Afghans and Americans. And I made it very clear to the Pakistanis that the attack on our embassy was an outrage and the attack on our forward operating base that injured 77 of our soldiers was a similar outrage.''.

(6) At the same hearing, Secretary of State Clinton further stated that ''I think everyone agrees that the Haqqani Network has safe havens inside Pakistan; that those safe havens give them a place to plan and direct operations that kill Afghans and Americans.''.

(7) On November 1, 2011, the United States Government added Haji Mali Kahn to a list of specially designated global terrorists under Executive Order 13224. The Department of State described Khan as ''a Haqqani Network commander'' who has ''overseen hundreds of fighters, and has instructed his subordinates to conduct terrorist acts.'' The designation continued, ''Mali Khan has provided support and logistics to the Haqqani Network, and has been involved in the planning and execution of attacks in Afghanistan against civilians, coalition forces, and Afghan police''. According to Jason Blazakis, the chief of the Terrorist Designations Unit of the Department of State, Khan also has links to al-Qaeda.

(8) Five other top Haqqani Network leaders have been placed on the list of specially designated global terrorists under Executive Order 13224 since 2008, and three of them have been so placed in the last year. Sirajuddin Haqqani, the overall leader of the Haqqani Network as well as the leader of the Taliban's Mira shah Regional Military Shura, was designated by the Secretary of State as a terrorist in March 2008, and in March 2009, the Secretary of State put out a bounty of $5,000,000 for information leading to his capture. The other four individuals so designated are Nasiruddin Haqqani, Khalil al Rahman Haqqani, Badruddin Haqqani, and Mullah Sangeen Zadran.

(b) SENSE OF CONGRESS.—It is the sense of Congress that—

(1) the Haqqani Network meets the criteria for designation as a foreign terrorist organization as set forth in section 219 of the Immigration and Nationality Act (8 U.S.C. 1189); and

(2) the Secretary of State should so designate the Haqqani Network as a foreign terrorist organization under such section 219.

(c) REPORT.—

(1) REPORT REQUIRED.—Not later than 30 days after the date of the enactment of this Act, the Secretary of State shall submit to the appropriate committees of Congress—

(A) a detailed report on whether the Haqqani Network meets the criteria for designation as a foreign terrorist organization as set forth in section 219 of the Immigration and Nationality Act (8 U.S.C. 1189); and

(B) if the Secretary determines that the Haqqani Network does not meet the criteria set forth under such section 219, a detailed justification as to which criteria have not been met.

(2) FORM.—The report required by paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(3) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this subsection, the term ''appropriate committees of Congress'' means—

(A) the Committee on Armed Services, the Committee on Foreign Relations, the Committee on the Judiciary, and the Select Committee on Intelligence of the Senate; and

(B) the Committee on Armed Services, the Committee on Foreign Affairs, the Committee on the Judiciary, and the Permanent Select Committee on Intelligence of the House of Representatives.

(d) CONSTRUCTION.—Nothing in this Act may be construed to infringe upon the sovereignty of Pakistan to combat militant or terrorist groups operating inside the boundaries of Pakistan.

Mr. SCHUMER. I make a motion to concur in the House amendment, and I know of no further debate on this measure.

The PRESIDING OFFICER. The question is on agreeing to the motion.

The motion was agreed to.

Mr. SCHUMER. I ask unanimous consent that the motion to reconsider be laid upon the table and that any statements relating to the bill be printed at this point in the RECORD.

The PRESIDING OFFICER. Without objection, it is so ordered.

LIONS CLUBS INTERNATIONAL CENTURY OF SERVICE COMMEMORATIVE COIN ACT

Mr. SCHUMER. I ask unanimous consent that the Committee on Banking, Housing, and Urban Affairs be discharged from further consideration of S. 1299 and that the Senate proceed to its immediate consideration.

The PRESIDING OFFICER. Without objection, it is so ordered. The clerk will report the bill by title.

The bill clerk read as follows:

A bill (S. 1299) to require the Secretary of the Treasury to mint coins in commemoration of the centennial of the establishment of Lions Clubs International.

There being no objection, the Senate proceeded to consider the bill.

Mr. SCHUMER. I ask unanimous consent that the bill be read a third time and passed, the motion to reconsider be laid upon the table, and that any statements relating to the bill be printed in the RECORD.

The PRESIDING OFFICER. Without objection, it is so ordered.

The bill (S. 1299) was ordered to be engrossed for a third reading, was read the third time, and passed, as follows:

S. 1299

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Lions Clubs International Century of Service Commemorative Coin Act''.

SEC. 2. FINDINGS.

The Congress finds as follows:

(1) Lions Clubs International is the world's largest service club organization founded in 1917 by Chicago business leader Melvin Jones. Lions Clubs International empowers volunteers to serve their communities, meet humanitarian needs, encourage peace and promote international understanding through Lions clubs.

(2) Today, Lions Clubs International has over 1.35 million members in more than 45,000 clubs globally, extending its mission of service throughout the world every day.

(3) In 1945, Lions Clubs International became one of the first nongovernmental organizations invited to assist in drafting the United Nations Charter and has enjoyed a special relationship with the United Nations ever since.

(4) In 1968, Lions Clubs International Foundation was established to assist with global and large-scale local humanitarian projects and has since then awarded more than $700 million to fund five unique areas of service: preserving sight, combating disability, promoting health, serving youth and providing disaster relief.

(5) In 1990, the Lions Clubs International Foundation launched the SightFirst program to build comprehensive eye care systems to fight the major causes of blindness and care for the blind or visually impaired. Thanks to the generosity of Lions worldwide, over $415 million has been raised, resulting in the prevention of serious vision loss in 30 million people and improved eye care for hundreds of millions of people.

(6) On June 7, 2017, Lions Clubs International will celebrate 100 years of community service to men, women, and children in need throughout the world.

SEC. 3. COIN SPECIFICATIONS.

(a) $1 SILVER COINS.—The Secretary of the Treasury (hereafter in this Act referred to as the ''Secretary'') shall mint and issue not more than 400,000 $1 coins in commemoration of the centennial of the founding of the Lions Clubs International, each of which shall—

(1) weigh 26.73 grams;

(2) have a diameter of 1.500 inches; and

(3) contain 90 percent silver and 10 percent copper.

(b) LEGAL TENDER.—The coins minted under this Act shall be legal tender, as provided in section 5103 of title 31, United States Code.

(c) NUMISMATIC ITEMS.—For purposes of sections 5134 and 5136 of title 31, United States Code, all coins minted under this Act shall be considered to be numismatic items.

SEC. 4. DESIGN OF COINS.

(a) DESIGN REQUIREMENTS.—

(1) IN GENERAL.—The design of the coins minted under this Act shall be emblematic of the centennial of the Lions Clubs International.

(2) DESIGNATION AND INSCRIPTIONS.—On each coin minted under this Act, there shall be—

(A) a designation of the value of the coin;

(B) an inscription of the year ''2017''; and

(C) inscriptions of the words ''Liberty'', ''In God We Trust'', ''United States of America'', and ''E Pluribus Unum''.

(b) SELECTION.—The design for the coins minted under this Act shall be—

(1) chosen by the Secretary after consultation with Lions Clubs International Special Centennial Planning Committee and the Commission of Fine Arts; and

(2) reviewed by the Citizens Coinage Advisory Committee.

SEC. 5. ISSUANCE OF COINS.

(a) QUALITY OF COINS.—Coins minted under this Act shall be issued in uncirculated and proof qualities.

(b) MINT FACILITY.—Only one facility of the United States Mint may be used to

strike any particular quality of the coins minted under this Act.

(c) PERIOD FOR ISSUANCE.—The Secretary may issue coins under this Act only during the calendar year beginning on January 1, 2017.

SEC. 6. SALE OF COINS.

(a) SALE PRICE.—The coins issued under this Act shall be sold by the Secretary at a price equal to the sum of—

(1) the face value of the coins;

(2) the surcharge provided in section 7 with respect to such coins; and

(3) the cost of designing and issuing the coins (including labor, materials, dies, use of machinery, overhead expenses, marketing, and shipping).

(b) BULK SALES.—The Secretary shall make bulk sales of the coins issued under this Act at a reasonable discount.

(c) PREPAID ORDERS.—

(1) IN GENERAL.—The Secretary shall accept prepaid orders for the coins minted under this Act before the issuance of such coins.

(2) DISCOUNT.—Sale prices with respect to prepaid orders under paragraph (1) shall be at a reasonable discount.

SEC. 7. SURCHARGES.

(a) IN GENERAL.—All sales of coins issued under this Act shall include a surcharge of $10 per coin.

(b) DISTRIBUTION.—Subject to section 5134(f) of title 31, United States Code, all surcharges received by the Secretary from the sale of coins issued under this Act shall be promptly paid by the Secretary to the Lions Clubs International Foundation for the purposes of—

(1) furthering its programs for the blind and visually impaired in the United States and abroad;

(2) investing in adaptive technologies for the disabled; and

(3) investing in youth and those affected by a major disaster.

(c) AUDITS.—The Comptroller General of the United States shall have the right to examine such books, records, documents, and other data of the Lions Clubs International Foundation as may be related to the expenditures of amounts paid under subsection (b).

(d) LIMITATION.—Notwithstanding subsection (a), no surcharge may be included with respect to the issuance under this Act of any coin during a calendar year if, as of the time of such issuance, the issuance of such coin would result in the number of commemorative coin programs issued during such year to exceed the annual 2 commemorative coin program issuance limitation under section 5112(m)(1) of title 31, United States Code. The Secretary may issue guidance to carry out this subsection.

PROSTATE CANCER AWARENESS IN AFRICAN-AMERICAN MEN

NATIONAL REGISTERED APPRENTICESHIP MONTH

TEAM USA AND THE 2012 OLYMPIC AND PARALYMPIC GAMES

Mr. SCHUMER. Mr. President, I ask unanimous consent that the Senate proceed to the immediate consideration en bloc of the following resolutions which were submitted earlier today: S. Res. 529, S. Res. 530, and S. Res. 531.

There being no objection, the Senate proceeded to consider the resolutions en bloc.

Mr. SCHUMER. I ask unanimous consent that the resolutions be agreed to, the preambles be agreed to, the motions to reconsider be laid upon the table en bloc with no intervening action or debate, and that any statements related to the resolutions be printed in the RECORD.

The PRESIDING OFFICER. Without objection, it is so ordered.

The resolutions were agreed to.

The preambles were agreed to.

The resolutions, with their preambles, read as follows:

S. RES. 529

Whereas the incidence of prostate cancer in African-American men is more than one and a half times higher than in any other racial or ethnic group in the United States;

Whereas African-American men have the highest mortality rate of any ethnic and racial group in the United States, dying at a rate that is approximately two and a half times higher than other ethnic and racial groups;

Whereas that rate of mortality represents the largest disparity of mortality rates in any of the major cancers;

Whereas prostate cancer can be cured with early detection and the proper treatment, regardless of the ethnic or racial group of the cancer patient;

Whereas African Americans are more likely to be diagnosed at an earlier age and at a later stage of cancer progression than all other ethnic and racial groups, leading to lower cure rates and lower chances of survival;

Whereas, for patients diagnosed early, studies show a 5-year survival rate of nearly 100 percent, but the survival rate drops significantly to 28 percent for patients diagnosed in late stages; and

Whereas recent genomics research has increased the ability to identify men at high risk for aggressive prostate cancer: Now, therefore, be it

Resolved, That the Senate—

(1) recognizes that prostate cancer has created a health crisis for African-American men;

(2) recognizes the importance of health coverage and access to care, as well as promoting informed decisionmaking between men and their doctors, taking into consideration the known risks and potential benefits of screening and treatment options for prostate cancer;

(3) urges Federal agencies to support—

(A) research to address and attempt to end the health crisis created by prostate cancer;

(B) efforts relating to education, awareness, and early detection at the grassroots level to end that health crisis; and

(C) the Office of Minority Health of the Department of Health and Human Services in focusing on improving health and healthcare outcomes for African Americans at an elevated risk of prostate cancer; and

(4) urges investment by Federal agencies in research focusing on the improvement of early detection and treatment of prostate cancer, such as the use of—

(A) biomarkers to accurately distinguish indolent forms of prostate cancer from lethal forms; and

(B) advanced imaging tools to ensure the best level of individualized patient care.

S. RES. 530

Whereas 2012 marks the 75th anniversary of the enactment of the Act of August 16, 1937 (29 U.S.C. 50 et seq.) (commonly known as the ''National Apprenticeship Act''), which established the national registered apprenticeship system;

Whereas the State of Wisconsin created the first State registered apprenticeship system in 1911;

Whereas the Act of August 16, 1937 (29 U.S.C. 50 et seq.) (commonly known as the ''National Apprenticeship Act'') established a comprehensive system of partnerships among employers, labor organizations, educational institutions, and Federal and State governments, which has shaped skill training for succeeding generations of United States workers;

Whereas for 75 years, the national registered apprenticeship system has provided state of the art training using an model known as ''earn while you learn'' that offers a pathway to the middle class and a sustainable career for millions of workers in the United States;

Whereas the national registered apprenticeship system has grown to include approximately 24,000 programs across the United States, providing education and training for apprentices in emerging and high-growth sectors, such as information technology and health care, as well as in traditional industries;

Whereas the national registered apprenticeship system leverages approximately $1,000,000,000 in private investment, reflecting the strong commitment of the sponsors of the system, which include industry associations, individual employers, and labor-management partnerships;

Whereas the national registered apprenticeship system is an important post-secondary pathway for United States workers, offering a combination of academic and technical instruction with paid, on-the-job training, resulting in a nationally and industry-recognized occupational credential that ensures higher earnings for apprentices and a highly skilled workforce for United States businesses;

Whereas the national registered apprenticeship system has continually modernized and developed innovative training approaches to meet the workforce needs of industry and address the evolving challenges of staying competitive in the global economy;

Whereas the national registered apprenticeship system of the 21st century, as envisioned by the Advisory Committee on Apprenticeship of the Secretary of Labor and administered as a partnership between the Federal Government and State apprenticeship programs, is positioned to produce the highly skilled workers the United States economy needs now and in the future; and

Whereas the celebration of National Registered Apprenticeship Month—

(1) honors the industries that use the registered apprenticeship model;

(2) encourages other industries that could benefit from the registered apprenticeship model to train United States workers using the model; and

(3) recognizes the role the national registered apprenticeship system has played in preparing United States workers for jobs with family-sustaining wages: Now, therefore, be it

Resolved, That the Senate—

(1) designates August 2012, as ''National Registered Apprenticeship Month'';

(2) celebrates the 101st anniversary of the enactment of the first State registered apprenticeship law; and

(3) celebrates the 75th anniversary of the enactment of the Act of August 16, 1937 (29 U.S.C. 50 et seq.) (commonly known as the ''National Apprenticeship Act'').

S. RES. 531

Whereas, for over 100 years, the Olympic Movement has built a more peaceful and better world by educating young people through

amateur athletics, bringing together athletes from many countries in friendly competition, and forging new relationships bound by friendship, solidarity, and fair play;

Whereas the 2012 Olympic Games will take place in London, England from July 27, 2012 to August 12, 2012, and the 2012 Paralympic Games will take place from August 29, 2012 to September 9, 2012;

Whereas, at the 2012 Olympic Games, over 200 nations will compete in over 300 events, and Team USA will compete in 246 events;

Whereas, at the 2012 Olympic Games, over 200 nations will compete in 39 disciplines, and Team USA will compete in 38 of those disciplines;

Whereas 529 Olympians and over 245 Paralympians will compete on behalf of Team USA in London, England;

Whereas Team USA has won 934 gold medals, 730 silver medals, and 643 bronze medals, totaling 2,307 medals over the past 25 Olympic Games;

Whereas the people of the United States stand united in respect and admiration for the members of the United States Olympic and Paralympic teams, and the athletic accomplishments, sportsmanship, and dedication to excellence of the teams;

Whereas the many accomplishments of the United States Olympic and Paralympic teams would not have been possible without the hard work and dedication of many others, including the United States Olympic Committee and the many administrators, coaches, and family members who provided critical support to the athletes;

Whereas the Nation takes great pride in the qualities of commitment to excellence, grace under pressure, and good will toward other competitors exhibited by the athletes of Team USA; and

Whereas the Olympic Movement celebrates competition, fair play, and the pursuit of dreams: Now, therefore, be it

Resolved, That the Senate—

(1) applauds all of the athletes and coaches of Team USA and their families who support them;

(2) supports the athletes of Team USA in their endeavors at the 2012 Olympic and Paralympic Games held in London, England;

(3) thanks all of the members of the United States Olympics Committee for their unwavering support of the athletes of Team USA; and

(4) supports the goals and ideals of the Olympic Games.

XIX INTERNATIONAL AIDS CONFERENCE

Mr. SCHUMER. Mr. President, I ask unanimous consent that the Senate proceed to the immediate consideration of S. Res. 532, submitted earlier today by Senator NELSON of Florida.

The PRESIDING OFFICER. The clerk will report the resolution by title.

The bill clerk read as follows:

A resolution (S. Res. 532) expressing support for the XIX International HIV/AIDS Conference and the sense of the Senate that continued commitment by the United States to research, prevention, and treatment programs is crucial to protecting global health.

There being no objection, the Senate proceeded to consider the resolution.

Mr. SCHUMER. I further ask unanimous consent that the Senate now proceed to a voice vote on the adoption of the resolution.

THE PRESIDING OFFICER. Without objection, it is so ordered.

The question is on agreeing to the resolution.

The resolution (S. Res. 532) was agreed to.

Mr. SCHUMER. Mr. President, I further ask unanimous consent that the preamble be agreed to, the motions to reconsider be made and laid upon the table, with no intervening action or debate, and that any statements relating to this matter be printed in the RECORD.

The PRESIDING OFFICER. Without objection, it is so ordered.

The preamble was agreed to.

The resolution (S. 532), with its preamble, reads as follows:

Whereas, according to UNAIDS, the Joint United Nations Programme on HIV/AIDS, there are approximately 33,400,000 people living with HIV worldwide, and nearly 30,000,000 people have died of AIDS since the first cases were reported in 1981;

Whereas, in the United States, more than 1,000,000 people are living with HIV and approximately 50,000 people become newly infected with the virus each year;

Whereas, according to the Centers for Disease Control and Prevention, 1 in 5 individuals living with HIV is unaware of the infection, underscoring the need for greater education about HIV/AIDS and access to testing;

Whereas societal stigma remains a significant challenge to addressing HIV/AIDS;

Whereas the United States is heavily engaged in both international and domestic efforts to address the HIV/AIDS pandemic, including—

(1) the United States President's Emergency Plan for AIDS Relief (commonly known as ''PEPFAR'');

(2) the Global Fund to Fight AIDS, Tuberculosis, and Malaria;

(3) title XXIV of the Public Health Service Act (42 U.S.C. 300dd et seq.) (originally enacted as part of the Ryan White Comprehensive AIDS Resources Emergency Act of 1990 (Public Law 101-381; 104 Stat. 576));

(4) State AIDS Drug Assistance Programs;

(5) the Housing Opportunities for Persons with AIDS program of the Department of Housing and Urban Development; and

(6) AIDS research at the National Institutes of Health and other agencies;

Whereas, since 1985, the now biennial International AIDS Conference has brought together leading scientists, public health experts, policymakers, community leaders, and individuals living with HIV/AIDS from around the world to enhance the global response to HIV/AIDS, evaluate recent scientific developments, share knowledge, and facilitate a collective strategy to combat the HIV/AIDS pandemic;

Whereas, in 2008, Congress passed and the President signed into law the Tom Lantos and Henry J. Hyde United States Global Leadership Against HIV/AIDS, Tuberculosis, and Malaria Reauthorization Act of 2008 (Public Law 110-293; 122 Stat. 2918);

Whereas taxpayers in the United States have paid more than $45,000,000,000 through PEPFAR and the Global Fund to Fight AIDS, Tuberculosis, and Malaria, which have enjoyed broad bipartisan support in Congress;

Whereas, 25 years after the III International AIDS Conference was held in Washington, D.C., the XIX International AIDS Conference (referred to in this preamble as ''AIDS 2012'') will take place from July 22, 2012, through July 27, 2012, at the Walter E. Washington Convention Center, in Washington, D.C.;

Whereas AIDS 2012, organized by the International AIDS Society, is expected to convene more than 20,000 delegates, including 2,000 journalists, from nearly 200 countries;

Whereas the theme of AIDS 2012, ''Turning the Tide Together'', embodies the promise and urgency of utilizing recent scientific advances in HIV/AIDS treatment and biomedical prevention, continuing research for an HIV vaccine and cure, and increasing effective, evidence-based interventions in key settings to change the course of the HIV/AIDS crisis;

Whereas AIDS 2012 seeks to engage governments, nongovernmental organizations, policymakers, the scientific community, the private sector, civil society, faith-based organizations, the media, and people living with HIV/AIDS to more effectively address regional, national, and local responses to HIV/AIDS around the world and overcome barriers that limit access to preventative care, treatment, and other services; and

Whereas AIDS 2012 is a tremendous opportunity to strengthen the role of the United States in global HIV/AIDS initiatives within the context of significant global economic challenges, reenergize the response to the domestic epidemic, and focus particular attention on the devastating impact of HIV/AIDS that continues in the United States: Now, therefore, be it

Resolved, That the Senate—

(1) supports the XIX International AIDS Conference and the goal of renewing awareness of, and commitment to, addressing the HIV/AIDS crisis in the United States and abroad;

(2) recognizes that continued HIV/AIDS research, prevention, and treatment programs are crucial to improving global health;

(3) understands that the key to overcoming HIV/AIDS includes efforts to formulate sound public health policy, protect human rights, address the needs of women and girls, direct effective programming toward the populations at the highest risk of infection, ensure accountability, and combat stigma, poverty, and other social challenges related to HIV/AIDS;

(4) seeks to work with all stakeholders—

(A) to prevent the transmission of HIV;

(B) to increase access to testing, treatment, and care;

(C) to improve health outcomes for all people living with HIV/AIDS; and

(D) to foster greater scientific and programmatic collaborations around the world to translate scientific advances and apply best practices to international efforts to end HIV/AIDS;

(5) commits to supporting a stronger global response to HIV/AIDS, protecting the rights of people living with HIV/AIDS, and working to create an ''AIDS-free generation''; and

(6) encourages the ongoing development in the public and private sectors of innovative therapies and advances in clinical treatment for HIV/AIDS, including—

(A) new and improved biomedical and behavioral prevention strategies;

(B) safer and more affordable, accessible, and effective treatment regimens for infected individuals; and

(C) research for an HIV vaccine and cure.

AUTHORIZING THE PRINTING OF THE 25TH EDITION OF THE POCKET VERSION OF THE UNITED STATES CONSTITUTION

Mr. SCHUMER. Mr. President, I ask unanimous consent that the Rules Committee be discharged from further consideration of H. Con. Res. 90 and the Senate proceed to its consideration.

The PRESIDING OFFICER. Without objection, it is so ordered.

The clerk will report the concurrent resolution by title.

The bill clerk read as follows:

A concurrent resolution (H. Con. Res. 90) authorizing the printing of the 25th edition of the pocket version of the United States Constitution.

There being no objection, the Senate proceeded to consider the concurrent resolution.

Mr. SCHUMER. I ask unanimous consent that the concurrent resolution be agreed to, the motion to reconsider be laid upon the table, with no intervening action or debate, and any statements related to the measure be printed in the RECORD.

The PRESIDING OFFICER. Without objection, it is so ordered.

The concurrent resolution (H. Con. Res. 90) was agreed to.

AUTHORIZING THE USE OF THE ROTUNDA

Mr. SCHUMER. Mr. President, I ask unanimous consent the Senate proceed to H. Con. Res. 133, which was received from the House and is at the desk.

The PRESIDING OFFICER. Without objection, it is so ordered.

The clerk will report the concurrent resolution by title.

The bill clerk read as follows:

A concurrent resolution (H. Con. Res. 133) authorizing the use of the rotunda of the United States Capitol for an event to present the Congressional Gold Medal to Arnold Palmer, in recognition of his service to the Nation in promoting excellence and good sportsmanship in golf.

There being no objection, the Senate proceeded to consider the concurrent resolution.

Mr. SCHUMER. I ask unanimous consent that the concurrent resolution be agreed to, the motion to reconsider be laid upon the table with no intervening action or debate, and any statements related to the measure be printed in the RECORD.

The PRESIDING OFFICER. Without objection, it is so ordered.

The concurrent resolution (H. Con. Res. 133) was agreed to.

CONDEMNING THE ATROCITIES IN AURORA, COLORADO

Mr. SCHUMER. Mr. President, I ask unanimous consent that the Senate proceed to the consideration of H. Con. Res. 134 just received from the House, and it is at the desk.

The PRESIDING OFFICER. The clerk will report the concurrent resolution by title.

The bill clerk read as follows:

A concurrent resolution (H. Con. Res. 134) condemning, in the strongest possible terms, the heinous atrocities that occurred in Aurora, Colorado.

There being no objection, the Senate proceeded to consideration of the concurrent resolution.

Mr. SCHUMER. Mr. President, I ask unanimous consent that the concurrent resolution be agreed to, the preamble be agreed to, the motion to reconsider be laid upon the table with no intervening action or debate, and that any statements be printed in the RECORD.

The PRESIDING OFFICER. Without objection, it is so ordered.

The concurrent resolution (H. Con. Res. 134) was agreed to.

The preamble was agreed to.

MEASURE READ THE FIRST TIME—H.R. 6082

Mr. SCHUMER. Mr. President, I understand there is a bill at the desk, and I ask for its first reading.

The PRESIDING OFFICER. The clerk will report the bill by title.

The bill clerk read as follows:

A bill (H.R. 6082) to officially replace, within the 60-day Congressional review period under the Outer Continental Shelf Lands Act, President Obama's Proposed Final Outer Continental Shelf Oil & Gas Leasing Program (2012–2017) with a congressional plan that will conduct additional oil and natural gas lease sales to promote offshore energy development, job creation, and increased domestic energy production to ensure a more secure energy future in the United States, and for other purposes.

Mr. SCHUMER. I ask for a second reading, and in order to place the bill on the calendar under the provisions of rule XIV, I object to my own request.

The PRESIDING OFFICER. Objection is heard. The bill will be read for a second time on the next legislative day.

ORDERS FOR MONDAY, JULY 30, 2012

Mr. SCHUMER. Mr. President, I ask unanimous consent that when the Senate completes its business today, it adjourn until 2 p.m. on Monday, July 30; that following the prayer and pledge, the Journal of proceedings be approved to date, the morning hour be deemed expired, and the time for the two leaders be reserved for their use later in the day; that the majority leader be recognized; and that at 4:30 p.m., the Senate proceed to executive session to consider the nomination of Robert Bacharach, of Oklahoma, to be U.S. circuit judge for the Tenth Circuit, with 1 hour of debate equally divided and controlled in the usual form prior to a cloture vote on the Bacharach nomination; further, that if cloture is not invoked on the Bacharach nomination, the Senate then resume legislative session and adopt the motion to proceed to S. 3414, the Cybersecurity Act; and finally, that if cloture is invoked on the Bacharach nomination, upon disposition of the nomination, the Senate resume legislative session and adopt the motion to proceed to S. 3414, the Cybersecurity Act.

The PRESIDING OFFICER. Without objection, it is so ordered.

PROGRAM

Mr. SCHUMER. Mr. President, the next rollcall vote will be a cloture vote at 5:30 p.m. on Monday on the Bacharach nomination. On Monday evening, we expect to begin consideration of the cybersecurity bill. We will work on an agreement on amendments to the bill.

ADJOURNMENT UNTIL MONDAY, JULY 30, 2012, AT 2 P.M.

Mr. SCHUMER. Mr. President, if there is no further business to come before the Senate, I ask unanimous consent that it adjourn under the previous order.

There being no objection, the Senate, at 7 p.m., adjourned until Monday, July 30, 2012, at 2 p.m.

CONFIRMATIONS

Executive nominations confirmed by the Senate July 26, 2012:

IN THE AIR FORCE

THE FOLLOWING AIR NATIONAL GUARD OF THE UNITED STATES OFFICERS FOR APPOINTMENT IN THE RESERVE OF THE AIR FORCE TO THE GRADE INDICATED UNDER TITLE 10, U.S.C., SECTIONS 12203 AND 12212:

To be brigadier general

COLONEL EDWARD E. METZGAR

THE FOLLOWING AIR NATIONAL GUARD OF THE UNITED STATES OFFICER FOR APPOINTMENT IN THE RESERVE OF THE AIR FORCE TO THE GRADE INDICATED UNDER TITLE 10, U.S.C., SECTIONS 12203 AND 12212:

To be brigadier general

COL. RUSS A. WALZ

THE FOLLOWING NAMED OFFICER FOR APPOINTMENT IN THE UNITED STATES AIR FORCE TO THE GRADE INDICATED UNDER TITLE 10, U.S.C., SECTION 624:

To be major general

BRIG. GEN. TIMOTHY M. RAY

THE FOLLOWING NAMED OFFICER FOR APPOINTMENT IN THE UNITED STATES AIR FORCE TO THE GRADE INDICATED WHILE ASSIGNED TO A POSITION OF IMPORTANCE AND RESPONSIBILITY UNDER TITLE 10, U.S.C., SECTION 601:

To be general

LT. GEN. PAUL J. SELVA

THE FOLLOWING NAMED OFFICER FOR APPOINTMENT AS THE VICE CHIEF OF THE NATIONAL GUARD BUREAU AND FOR APPOINTMENT TO THE GRADE INDICATED IN THE RESERVE OF THE AIR FORCE UNDER TITLE 10, U.S.C., SECTIONS 10505 AND 601:

To be lieutenant general

MAJ. GEN. JOSEPH L. LENGYEL

THE FOLLOWING NAMED OFFICER FOR APPOINTMENT IN THE UNITED STATES AIR FORCE TO THE GRADE INDICATED UNDER TITLE 10, U.S.C., SECTION 624:

To be major general

BRIG. GEN. HOWARD D. STENDAHL

IN THE ARMY

THE FOLLOWING NAMED OFFICER FOR APPOINTMENT IN THE RESERVE OF THE ARMY TO THE GRADE INDICATED UNDER TITLE 10, U.S.C., SECTION 12203:

To be major general

BRIG. GEN. LAWRENCE W. BROCK

THE FOLLOWING ARMY NATIONAL GUARD OF THE UNITED STATES OFFICER FOR APPOINTMENT IN THE RESERVE OF THE ARMY TO THE GRADE INDICATED UNDER TITLE 10, U.S.C., SECTIONS 12203 AND 12211:

To be major general

BRIG. GEN. REYNOLD N. HOOVER

THE FOLLOWING NAMED OFFICER FOR APPOINTMENT IN THE UNITED STATES ARMY TO THE GRADE INDICATED WHILE ASSIGNED TO A POSITION OF IMPORTANCE AND RESPONSIBILITY UNDER TITLE 10, U.S.C., SECTION 601:

To be lieutenant general

MAJ. GEN. JAMES O. BARCLAY III

THE FOLLOWING NAMED OFFICER FOR APPOINTMENT IN THE UNITED STATES ARMY TO THE GRADE INDICATED WHILE ASSIGNED TO A POSITION OF IMPORTANCE AND RESPONSIBILITY UNDER TITLE 10, U.S.C., SECTION 601:

To be lieutenant general

LT. GEN. DONALD M. CAMPBELL, JR.

THE FOLLOWING NAMED OFFICER FOR APPOINTMENT AS THE CHIEF OF THE NATIONAL GUARD BUREAU AND

FOR APPOINTMENT TO THE GRADE INDICATED IN THE RESERVE OF THE ARMY UNDER TITLE 10, U.S.C., SECTIONS 10502 AND 601:

To be general

LT. GEN. FRANK J. GRASS

THE FOLLOWING NAMED OFFICER FOR APPOINTMENT IN THE UNITED STATES ARMY TO THE GRADE INDICATED WHILE ASSIGNED TO A POSITION OF IMPORTANCE AND RESPONSIBILITY UNDER TITLE 10, U.S.C., SECTION 601:

To be lieutenant general

MAJ. GEN. DAVID R. HOGG

THE FOLLOWING ARMY NATIONAL GUARD OF THE UNITED STATES OFFICER FOR APPOINTMENT IN THE RESERVE OF THE ARMY TO THE GRADE INDICATED UNDER TITLE 10, U.S.C., SECTIONS 12203 AND 12211:

To be major general

BRIG. GEN. JOYCE L. STEVENS

IN THE NAVY

THE FOLLOWING NAMED OFFICER FOR APPOINTMENT IN THE UNITED STATES NAVY TO THE GRADE INDICATED WHILE ASSIGNED TO A POSITION OF IMPORTANCE AND RESPONSIBILITY UNDER TITLE 10, U.S.C., SECTION 601:

To be vice admiral

VICE ADM. ALLEN G. MYERS

THE FOLLOWING NAMED OFFICERS FOR APPOINTMENT IN THE UNITED STATES NAVY TO THE GRADE INDICATED UNDER TITLE 10, U.S.C., SECTION 624:

To be rear admiral (lower half)

CAPTAIN JOHN D. ALEXANDER
CAPTAIN BRET C. BATCHELDER
CAPTAIN RONALD A. BOXALL
CAPTAIN ROBERT P. BURKE
CAPTAIN DAVID J. HAHN
CAPTAIN ALEXANDER L. KRONGARD
CAPTAIN ANDREW L. LEWIS
CAPTAIN BRUCE H. LINDSEY
CAPTAIN DEE L. MEWBOURNE
CAPTAIN JOHN P. NEAGLEY
CAPTAIN PATRICK A. PIERCEY
CAPTAIN MARKHAM K. RICH
CAPTAIN CHARLES A. RICHARD
CAPTAIN CYNTHIA M. THEBAUD
CAPTAIN BRAD WILLIAMSON
CAPTAIN RICKY L. WILLIAMSON

THE FOLLOWING NAMED OFFICER FOR APPOINTMENT TO THE GRADE OF ADMIRAL IN THE UNITED STATES NAVY WHILE ASSIGNED TO A POSITION OF IMPORTANCE AND RESPONSIBILITY UNDER TITLE 10, U.S.C., SECTION 601 AND TITLE 42, U.S.C., SECTION 7158:

TO BE DIRECTOR, NAVAL NUCLEAR PROPULSION PROGRAM

To be admiral

VICE ADM. JOHN M. RICHARDSON

THE FOLLOWING NAMED OFFICER FOR APPOINTMENT IN THE UNITED STATES NAVY TO THE GRADE INDICATED WHILE ASSIGNED TO A POSITION OF IMPORTANCE AND RESPONSIBILITY UNDER TITLE 10, U.S.C., SECTION 601:

To be vice admiral

REAR ADM. DAVID A. DUNAWAY

IN THE MARINE CORPS

THE FOLLOWING NAMED OFFICER FOR APPOINTMENT TO THE GRADE OF GENERAL IN THE UNITED STATES MARINE CORPS WHILE ASSIGNED TO A POSITION OF IMPORTANCE AND RESPONSIBILITY UNDER TITLE 10, U.S.C., SECTION 601:

To be general

LT. GEN. JOHN F. KELLY

IN THE AIR FORCE

AIR FORCE NOMINATIONS BEGINNING WITH JOLENE A. AINSWORTH AND ENDING WITH DAVID C. ZIMMERMAN, WHICH NOMINATIONS WERE RECEIVED BY THE SENATE AND APPEARED IN THE CONGRESSIONAL RECORD ON APRIL 23, 2012.

AIR FORCE NOMINATIONS BEGINNING WITH UCHENNA L. UMEH AND ENDING WITH DANIEL X. CHOI, WHICH NOMINATIONS WERE RECEIVED BY THE SENATE AND APPEARED IN THE CONGRESSIONAL RECORD ON JUNE 25, 2012.

AIR FORCE NOMINATIONS BEGINNING WITH CATHERINE M. FAHLING AND ENDING WITH LE T. ZIMMERMAN, WHICH NOMINATIONS WERE RECEIVED BY THE SENATE AND APPEARED IN THE CONGRESSIONAL RECORD ON JUNE 25, 2012.

AIR FORCE NOMINATIONS BEGINNING WITH SEAN J. HISLOP AND ENDING WITH LUCAS P. NEFF, WHICH NOMINATIONS WERE RECEIVED BY THE SENATE AND APPEARED IN THE CONGRESSIONAL RECORD ON JULY 17, 2012.

IN THE ARMY

ARMY NOMINATION OF KAREN A. BALDI, TO BE COLONEL.

ARMY NOMINATION OF CHRISTOPHER W. SOIKA, TO BE COLONEL.

ARMY NOMINATION OF LUIS A. RIVERABERRIOS, TO BE COLONEL.

ARMY NOMINATION OF KIMON A. NICOLAIDES, TO BE COLONEL.

ARMY NOMINATIONS BEGINNING WITH PENNY P. KALUA AND ENDING WITH JOSEPH A. TRINIDAD, WHICH NOMINATIONS WERE RECEIVED BY THE SENATE AND APPEARED IN THE CONGRESSIONAL RECORD ON JUNE 25, 2012.

ARMY NOMINATIONS BEGINNING WITH CHAD S. ABBEY AND ENDING WITH JARED K. ZOTZ, WHICH NOMINATIONS WERE RECEIVED BY THE SENATE AND APPEARED IN THE CONGRESSIONAL RECORD ON JULY 17, 2012.

ARMY NOMINATIONS BEGINNING WITH JEFFREY E. AYCOCK AND ENDING WITH ERIC W. YOUNG, WHICH NOMINATIONS WERE RECEIVED BY THE SENATE AND APPEARED IN THE CONGRESSIONAL RECORD ON JULY 17, 2012.

ARMY NOMINATIONS BEGINNING WITH BRENT A. BECKLEY AND ENDING WITH STEPHEN J. WARD, WHICH NOMINATIONS WERE RECEIVED BY THE SENATE AND APPEARED IN THE CONGRESSIONAL RECORD ON JULY 17, 2012.

ARMY NOMINATION OF BRIAN J. EASTRIDGE, TO BE COLONEL.

IN THE NAVY

NAVY NOMINATIONS BEGINNING WITH JOEL A. AHLGRIM AND ENDING WITH MARK L. WOODBRIDGE, WHICH NOMINATIONS WERE RECEIVED BY THE SENATE AND APPEARED IN THE CONGRESSIONAL RECORD ON JULY 11, 2012.

NAVY NOMINATIONS BEGINNING WITH JOHN E. BISSELL AND ENDING WITH STEPHEN S. YUNE, WHICH NOMINATIONS WERE RECEIVED BY THE SENATE AND APPEARED IN THE CONGRESSIONAL RECORD ON JULY 11, 2012.

NAVY NOMINATIONS BEGINNING WITH ROBERT L. ANDERSON II AND ENDING WITH CAROL B. ZWIEBACH, WHICH NOMINATIONS WERE RECEIVED BY THE SENATE AND APPEARED IN THE CONGRESSIONAL RECORD ON JULY 11, 2012.

NAVY NOMINATIONS BEGINNING WITH MARC S. BREWEN AND ENDING WITH DUSTIN E. WALLACE, WHICH NOMINATIONS WERE RECEIVED BY THE SENATE AND APPEARED IN THE CONGRESSIONAL RECORD ON JULY 11, 2012.

NAVY NOMINATIONS BEGINNING WITH LUCELINA B. BADURA AND ENDING WITH WILLIAM A. YOUNG, WHICH NOMINATIONS WERE RECEIVED BY THE SENATE AND APPEARED IN THE CONGRESSIONAL RECORD ON JULY 11, 2012.

NAVY NOMINATIONS BEGINNING WITH JASON W. ADAMS AND ENDING WITH SHAWN M. TRIGGS, WHICH NOMINATIONS WERE RECEIVED BY THE SENATE AND APPEARED IN THE CONGRESSIONAL RECORD ON JULY 11, 2012.

NAVY NOMINATIONS BEGINNING WITH DAVID L. CLINE AND ENDING WITH DAVID S. YANG, WHICH NOMINATIONS WERE RECEIVED BY THE SENATE AND APPEARED IN THE CONGRESSIONAL RECORD ON JULY 11, 2012.

NAVY NOMINATIONS BEGINNING WITH EMILY Z. ALLEN AND ENDING WITH JONATHAN P. WITHAM, WHICH NOMINATIONS WERE RECEIVED BY THE SENATE AND APPEARED IN THE CONGRESSIONAL RECORD ON JULY 11, 2012.