United States of America

Congressional Record

PROCEEDINGS AND DEBATES OF THE 112th CONGRESS, SECOND SESSION

Vol. 158 WASHINGTON, MONDAY, JULY 30, 2012 *No. 114*

Senate

The Senate met at 2 p.m. and was called to order by the Honorable MARK R. WARNER, a Senator from the Commonwealth of Virginia.

PRAYER

The Chaplain, Dr. Barry C. Black, offered the following prayer:

Let us pray.

Eternal Savior, our God and our strength, in the shadow of Your hand, we find protection from life's slings and arrows. You keep us from toiling in vain, from spending our strength for nothing. Today, use our lawmakers to make America a light of the nations. May our Senators work with such integrity and dependence on You that freedom may reach to the end of the Earth. Lord, help them to seek first and foremost to know and do Your will and reward them for their service and sacrifices for freedom. Have compassion on us all and guide us to the springs of living water.

We pray in Your merciful Name. Amen.

PLEDGE OF ALLEGIANCE

The Honorable MARK R. WARNER 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 bill clerk read the following letter.

U.S. SENATE,
PRESIDENT PRO TEMPORE,
Washington, DC, July 30, 2012.

To the Senate:

Under the provisions of rule I, paragraph 3, of the Standing Rules of the Senate, I hereby appoint the Honorable MARK R. WARNER, a Senator from the Commonwealth of Virginia, to perform the duties of the Chair.

DANIEL K. INOUYE,
President pro tempore.

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

CYBERSECURITY ACT OF 2012—MOTION TO PROCEED

RECOGNITION OF THE MAJORITY LEADER

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

SCHEDULE

Mr. REID. Mr. President, we are on the motion to proceed to S. 3414, which is the cybersecurity bill. This is postcloture. At 4:30 p.m., the Senate will proceed to executive session to vote on the nomination of Robert Bacharach, of Oklahoma, to be a U.S. circuit judge for the Tenth Circuit. This likely will be our last vote on a circuit judge for this Congress. I hope we can be successful. This is a person whom I will talk about a little bit, and he is certainly well qualified. He came out of committee unanimously.

At 5:30 p.m., today, there will be a cloture vote on the Bacharach nomination. If cloture is not invoked on the Bacharach nomination, the Senate will resume legislative session and begin consideration of the cybersecurity bill following the vote.

MEASURE PLACED ON THE CALENDAR—H.R. 6082

I am told H.R. 6082 is at the desk and due for a second reading.

The ACTING PRESIDENT pro tempore. The clerk will report the bill by title.

The assistant 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. REID. Mr. President, I object to any further proceedings with regard to this bill.

The ACTING PRESIDENT pro tempore. Objection is heard. The bill will be placed on the calendar.

MIDDLE-CLASS TAX CUT

Mr. REID. Mr. President, I was glad to hear Speaker BOEHNER say last week he will bring the Senate-passed middle-class tax cut to the House floor for a vote. I heard again today he is going to hold to what he said. I think that is very good.

Our struggling Nation is one vote away from avoiding the fiscal cliff for middle-class families. Every Member of the House of Representatives should have an opportunity to show where they stand: with millionaires or the middle class. Members can support the Democrats' plan to cut taxes for 98 percent of Americans while reducing the deficit by almost $1 trillion or they can support the Republican plan to hand out more tax breaks to millionaires and billionaires, increasing taxes for 25 million American families struggling to put kids through college or even food on the table.

The two approaches demonstrate a glaring difference in priorities. There is another difference between the two plans. The Democrats' proposal is the only one with a chance of becoming law. President Obama said he would sign it tomorrow. What he will not do is sign into law any more wasteful giveaways to the wealthiest 2 percent.

The Senate has defeated the Republican proposal in a bipartisan vote, so it is simply a waste of time for House Republicans to continue to pursue their middle-class tax hike. House Republicans should stop holding the middle class hostage to extract more tax cuts for the richest of the rich. They

should pass our middle-class tax cut now. American families cannot afford to wait until the last moment to find out how their bottom line will look come January 1. People are sitting around their kitchen tables now trying to figure out whether they can afford to buy a home or rent a home, should they send their kids to college or trade school or should they or can they retire? Republicans shouldn't force 114 million families to guess whether they will have $1,600 less to spend or save next year. They certainly need to do something and do it now, and one simple vote can give them that certainty.

Mr. President, cybersecurity is basically a new word. Today, the Senate also continues to work to address this problem. This is a problem that national security experts call the most urgent threat to our country; that is, weakness in our defense against cybersecurity. Cyber terrorism could cripple the computer networks that control our electrical grid, water supplies, sewers, nuclear plants, energy pipelines, transportation networks, communications equipment, and financial systems, to name a few. GEN Martin Dempsey, chairman of the Joint Chiefs of Staff, said: ''A cyber attack could stop this society in its tracks.'' Cyber espionage does not just threaten our national security, it threatens our economic security as well. Hackers have already attacked one of the most important businesses we have in America today, the Nasdaq stock exchange. Major corporations are under attack every day, spending millions and millions of dollars to protect against cyber attacks. These attacks cost our economy billions of dollars a year and thousands of jobs.

GEN James Clapper, Director of National Intelligence, said Chinese cyber theft of American intellectual property is ''the greatest pillaging of wealth in history.''

''That's our future disappearing in front of us,'' added GEN Keith Alexander, Director of the National Security Administration.

In a report released last year, the American Chamber of Commerce said the government and private sector should work together to develop incentives for businesses to voluntarily act to protect our Nation's critical infrastructure. The legislation before this body today does exactly that. It establishes a public-private partnership to make our Nation safer and protect American jobs. I hope the Chamber will join in our efforts to pass this important legislation.

I personally believe this bill could go further to address the critical infrastructure, such as the networks operating our electrical grid, our water supply, and other life-sustaining systems. It is a tremendously important first step.

I applaud Senators LIEBERMAN, COLLINS, FEINSTEIN, and ROCKEFELLER for their work on this legislation. The bill managers are compiling a list of relevant amendments for consideration. I hope we can cooperate to work through the list and pass this legislation this week. We can't afford to fail to address what experts have called the greatest security challenge since the dawn of the nuclear age.

BACHARACH NOMINATION

I said I would talk a little bit about Judge Bacharach, and I intend to do that now.

Today, the Senate will vote on whether to end a filibuster of Judge Robert Bacharach, a nominee from Oklahoma to the Tenth Circuit Court of Appeals. By any measure, this man is the type of noncontroversial nominee the Senate would routinely confirm with broad bipartisan support. He was reported out of the Judiciary Committee by voice vote. Everybody said he is a good guy. He has the support of two Republican Senators from his State of Oklahoma. Senator COBURN, the junior Senator from Oklahoma, said Friday that Judge Bacharach is a stellar candidate and ought to get through.

Yet Republicans have signaled they are going to block his nomination. If they hold up this consensus candidate, it will be the first time an appeals court nominee with this bipartisan support has ever been filibustered on the floor.

Why should we ever be surprised? We have already had 85 filibusters, so we can add another one to it. I hope they don't filibuster this good man. I have already said this would be our last circuit court judge. It is too bad that is the case.

If Senator COBURN and Senator INHOFE broadly support this qualified nomination, blatant partisanship will be to blame. Senator COBURN said Judge Bacharach is ''an awfully good candidate caught in election-year politics.''

Will the Chair announce the business of the day.

RESERVATION OF LEADER TIME

The ACTING PRESIDENT pro tempore. Under the previous order, the leadership time is reserved.

Mr. REID. Mr. President, I note the absence of a quorum.

The ACTING PRESIDENT pro tempore. The clerk will call the roll.

The assistant bill clerk proceeded to call the roll.

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

The ACTING PRESIDENT pro tempore. Without objection, it is so ordered.

HIGHER EDUCATION

Mr. HARKIN. Mr. President, 2 years ago, not long after I became chairman of the Senate's Health, Education, Labor, and Pensions Committee, I made the decision to undertake an investigation of the for-profit sector of higher education.

My reason for doing so was compelling: Congress had just finished making huge new investments in the Pell grant program; meanwhile, enrollment in for-profit colleges had increased 225 percent over the previous 10 years compared to 31 percent for the rest of higher education.

So this is what we were looking at, as shown on this chart. The enrollment in the for-profit sector kept going up, and finally, in 2006, it took a huge increase—up from 765,000 in 2001 to 2.5 million, almost, in 2010. So while students at for-profit colleges made up between 10 and 13 percent of all the students, for-profit colleges now were receiving almost 25 percent of all student loans and Pell grants.

Meanwhile, troubling reports began to surface: prospective students being lied to by aggressive recruiters; other recruiters showing up at wounded warrior facilities and homeless shelters; students saddled with a mountain of debt, unable to find jobs.

Two years later, our investigation is complete. The committee has held 6 hearings, issued 30 document requests, compiled data from multiple agencies, interviewed many former students and employees, and compiled a fact-based authoritative public record.

Earlier today, we announced the release of our final report called ''For-Profit Higher Education: The Failure to Safeguard the Federal Investment and Ensure Student Success.''

This report provides a detailed explanation of how Congress has failed to properly monitor student outcomes in this sector of higher education or to safeguard the enormous investment taxpayers are making.

As this next chart shows, Pell grants going to the for-profit sector have grown from $2.5 billion to $8.8 billion, in just 5 years. Again, this is what we are looking at. Just think, that we had to do something; and look at this: $2.5 billion, up to $8.8 billion, in 5 years. These are Pell grants. As I said, about 10 percent of the students, 25 percent of all the Pell grants. This was twice as fast as anything else in higher education.

As the chairman of the Appropriations subcommittee that funds Pell grants, we work very hard to make sure Pell grants keep up, that we increase them. So it was distressing and outrageous to learn that a disproportionate share of this Federal investment is going to schools that are raking in big profits but failing to educate our students.

I will now put up another chart.

You have to ask the question: Has the American taxpayer gotten an acceptable return on this huge investment in students attending school in the for-profit sector? The answer is a resounding no.

More than half of the students who enrolled in 2008 and 2009 had withdrawn by 2010. At many of them, as the chart shows, the withdrawal rate was 67 percent, as shown here for Ashford University.

What this means is, for students who signed up at one of these schools and

got a loan, got a Pell grant, 1 year later 50 percent of them were not there. It was as high as 67 percent of students at Bridgepoint, Ashford University, who were not there.

So you say: Well, what happened to the money? Guess what. Bridgepoint got the Pell grant. Bridgepoint got the Stafford loan. The student dropped out, and the student has the debt.

The student has the debt, and the student has nothing to show for it: no appreciable skill, no diploma, nothing. In fact, they are worse off than when they started because now they have a huge debt hanging around their neck. I just want to say that in this report, what we will find is overwhelming documentation of exorbitant tuition, unsavory recruiting practices, abysmal student outcomes, taxpayer dollars spent excessively on marketing and pocketed as profits, and regulatory evasion—regulatory evasion and manipulation.

I will have more to say about that later. Again, these practices are not the exception, they are the norm. They are systemic throughout the industry. There are, of course, individual exceptions. Again, there are real differences among the various for-profit colleges. That is why we took profiles of 30 different companies. We took 15 that were publicly owned, investor owned, and we took 15 that are more private. We took some from the biggest to the smallest so we would have a broad picture of what was happening in this industry.

Now, again, compared to the industry overall, some for-profit colleges are doing a better job for their students. I would mention Strayer, Walden, National American University, and American Public University—all private, for-profit schools doing a much better job for their students.

There are also for-profit colleges that have had serious shortcomings. But they are beginning to make some changes. They are now open to new thinking about how to improve student outcomes. I would include in this list Kaplan, DeVry, and Apollo, which is basically the University of Phoenix. The bottom line is that a large share of the $32 billion that taxpayers invested in these schools in 2010 was wasted. We cannot allow this to continue.

Why? Because 73 percent of undergraduate students in this country are nontraditional students. For example, they are holding down jobs, they are older, perhaps they have family responsibilities, come from maybe low-income communities, and they may be the first in their family to attend college. Our Nation's existing network of public and not-for-profit colleges and community colleges cannot meet the demand for higher education or meet President Obama's goal of producing more college graduates without increasing the number of Americans who spend at least some time in higher education. We need for-profit schools to offer these students more than a path to enrollment. We need them to offer students a path to success and graduation.

We uncovered two overall problems with the status quo in for-profit higher education. One, billions of taxpayer dollars are being diverted from the educational activities they were intended to finance; and, two, taxpayer dollars are being used to do real lasting harm to the students these colleges enroll.

Again, think about it. In just the 1 year we examined, more than half a million students enrolled in for-profit colleges and then quit. Almost every one of those dropouts left school worse off than when they began, with no tangible economic benefit, but saddled with debt that cannot be discharged in bankruptcy, far less able now to continue their higher education in the future because they will have defaulted on those loans. They will not be able to get Federal loans, and they will not get any more Pell grants.

So we have to ask why is this happening? One of the reasons is that the tuition at for-profit colleges is grossly out of line with the cost of comparable programs at public and nonprofit institutions and fail to reflect the often dubious value of a degree from a for-profit. As this chart shows, this is average, from a public college in yellow, and the purple is for-profit colleges.

For an average certificate program, public schools, $4,249—this is tuition. At a for-profit, $19,806; for an average associate degree, 2 years, $8,000 in public schools; that would be our community colleges and others, $34,988—almost $35,000 at a for-profit school. For a bachelor's degree, $52,000 in public schools; $62,000 in the for-profit schools. It costs 20 percent more for an online degree from Ashford University than a degree from the University of Michigan.

Now, since these schools do not have bricks and mortar, they do not have to pay heating bills and cooling bills and upkeep of dorms and all of that kind of stuff, one would think they could offer these courses much cheaper than what they are doing. That is not the case. They are much more expensive.

So why doesn't this lower overhead translate into lower tuition? We will put up the next chart. The answer is the efficiencies of online education are not passed on to students. Instead, those lower costs of delivery go straight to profits, marketing, and executive salaries. Tuition is set primarily based on maximizing revenue from Federal taxpayer dollars and on what executives think the market will bear.

That is sort of what this chart shows. This red line is the average available Federal aid to a student. This would be Stafford loans and Pell grants. This is average, $13,205. When we examined all of the private schools—this is just a representative sample—they are all just above that line. In fact, we have internal documents from many of these schools, from their executives, saying they are going to set their tuition in order to make sure they can maximize access to those Federal dollars.

Now, there are exceptions. I wanted to put one in there. American Public Institute, as I said earlier, they are way down here. They made a profit, they are profitable, and they provide a good service. They are not pegging their tuition costs at just what they can maximize. So there are examples out there, but the vast majority set it just at what the market will bear and how they can maximize their Federal dollars.

How much are these Federal dollars? About 83 percent. So I think another feature of the for-profit schools is their almost total reliance on taxpayer money. They say they are for-profit, but it is not like a for-profit for a private business that is competing in selling cars or washing machines or refrigerators or maybe some other kind of a service where one can pick and choose. About 83 percent—this is military, 3.8 percent, and 79.3 percent is Federal student aid dollars; 83 percent comes directly from the taxpayers of this country.

So if for-profit colleges charge exorbitant tuition and often provide an inferior education while experiencing sky-high dropout rates, how are they able to recruit a steady stream of new students? The answer is that for-profit colleges are what I would call a marketing machine. They spend 42.1 percent of their revenues on marketing, recruiting, and profit. Yet they only spend 17 percent of revenues on actual instruction.

By comparison, the University of North Carolina System spends less than 2 percent of its budget on marketing—2 percent. What we see is 42 percent—42 percent on marketing and profits; 17 percent on student instruction. This is interesting: 40.7 percent all other spending. I would point out herein are executive salaries, executive compensation, bonuses paid to recruiters, and on and on and on. Only 17 percent for instruction.

Most colleges, when they talk about marketing, it is down around 2 or 3 percent. I will bet the University of Virginia is probably down there. I do not know. We may have that documentation. I know the University of Iowa System is down around that 2- to 3-percent total for marketing. You have seen their ads, different things for public universities, nonprofit universities, but nothing close to 42 percent.

This is what leads to what we call the ''churn.'' Students come in, they get recruited, they get their Pell grants, they get their loans, the school gets the money, a year later the student drops out, and so the marketers go out and bring in more students. So we get this tremendous churn in the student body at these for-profit schools. Perhaps most critical, these institutions fail to provide adequate student support services, as I said. This is a critical finding of our report.

Despite knowingly enrolling some of the most at-risk students in our country, many of these schools do not provide these students with the services common sense tells us they need to succeed. How many times have we heard from the for-profit industry: Yes, we are different because we are enrolling students who do not go to our normal colleges, do not go to the University of Iowa, to the University of Virginia. These are nontraditional students. Many of them are poor. That is true, but that is who they are recruiting.

Why are they recruiting them? To get the most Pell grants and the most Stafford student loans. That is what the college gets.

Now, if they are doing that, then they need to provide mentoring, tutoring, some kind of alumni network, job partnerships, and genuine career counseling. Two of the largest for-profit companies provide no career counseling or placement to students whatsoever. Yet these are the very students who need the most help when they go to college. Students from upper income families who go to good schools, they do not need that. English language learners, Latinos, African-American students, those we intuitively know need more education. Maybe they have lost a job and now they realize: I have to do something. I have to get a better education. These marketers go after them. This is what our report found.

If you look at the enrollment in these schools, as I said, it has gone up. The enrollment has gone up. Look at the recruiters. From 2007 to 2010, we went from a little over 20,000 to 35,202 recruiters at 24 of these companies.

Down here, the red line, these are the career services. These are the people who counsel and mentor and tutor and help with career guidance. It has not gone up a bit. Huge increase in students, big increase in recruiters, and almost no increase at all in career counselors. This is a failure, an abject failure.

This report is the first comprehensive fact-based analysis of this industry. Earlier today I saw that the association for for-profit institutions called this a flawed process. As near as I can understand their critique, the process was flawed because it was about them, but that is what congressional oversight is about.

This was not an overnight thing. This is what we produced: four huge volumes, data-driven documentation, documentation on what is happening in this industry. This is the summary. This holds most of what we found. These three will have all of the backup documentation that is needed to support the findings we have.

We have before us a factual record that we have never had before. The Department of Education did not have it. No one has had it before. This can guide us as we move toward reauthorization of the Higher Education Act next year. Again, during the reauthorization we will also be looking at traditional higher education.

We have already held two hearings on college affordability. There is no question that we need to find a way to improve outcomes not just at for-profit colleges but also at low-cost community colleges. That said, the fact is there are problems that are unique—unique to the for-profit sector that will require some unique solutions.

We have seen some progress on this front, as I said. I have met with some of them. They have expressed a determination to reform and to do right by their students. In addition, the Department of Education took steps that are beginning to have real impacts.

In April, President Obama issued an Executive order that will help to ensure our veterans are not the subject of deceptive and misleading recruiting, and that will help solders and veterans to make better decisions about where to use their GI bill dollars.

Last month, Kentucky Attorney General Jack Conway led a 20-State attorney general settlement with QuinStreet, one of the companies engaged in some of the most egregiously misleading recruiting efforts targeted at veterans. But these are not enough. As I said, there is an important role for for-profit colleges in our increasingly knowledge-based economy.

A solid record of student success is in the national interest. The challenge is to require the companies to be as focused on student success as they are on financial success.

Now, there are four things we need to do.

First, we need to know how every student enrolled in college is doing, not just first-time, full-time students. This is a flaw in our system. The Department of Education only tracks first-time, full-time students. Most of the students who go to our for-profit schools are not first-time, full-time students, they are part-time students. So what we need to do is that for any student who gets a Pell grant and/or Stafford loan, we need to know how that student is doing and how they do later on.

Second, we need to be very clear that the Federal education money has to be spent on education, not advertising, recruiting, or lobbying. That is just common sense. I challenge anyone to stand up here and say: No, they should use taxpayer dollars to lobby, to advertise, or to pay a recruiter. No. We have to be very clear—they can spend it on education but not on advertising, recruiting or lobbying.

Third, we need to make sure these schools are providing at least a basic level of student services that would give the at-risk students they enroll a fair shot at completing. If there is one thing that distinguishes good for-profit schools from the bad ones, this is it: a genuine commitment to providing a network of student support—mentoring, tutoring, employer partnerships, genuine career counseling—not just in the beginning but all the way through the program. The good schools that are doing that are turning out quality products.

Fourth, we have to think seriously about outcome-based thresholds, particularly for colleges that get a very high proportion of their revenue from taxpayers. And we need to build on the gainful employment rule to ensure that students are not being loaded up with debt they cannot repay.

I am confident the record we are laying out today will make some of these reforms inevitable as we move forward. I wish to also thank some of my colleagues and to note that work has already begun on legislation.

Senator HAGAN is sponsoring a bill to ban the use of Federal financial aid dollars for marketing.

Senators MURRAY and WEBB are sponsoring comprehensive legislation to better protect servicemembers and veterans using the post-9/11 GI bill.

Senator LAUTENBERG is sponsoring a bill to provide every veteran who receives education aid from the Department of Veterans Affairs with counseling to help make the right choices and to create a system to track veterans' complaints of waste, fraud, and abuse by these for-profit schools.

Senators CARPER and DURBIN are sponsoring bills to address the absurdity of not counting all Federal money in the restriction on how much money these schools can receive.

One of the things we picked up on as we started this investigation was the tremendous focus these for-profits were now making on veterans, especially Iraq and Afghanistan veterans, and Active-Duty personnel. The reason for that is because we have a 90–10 rule that says for-profit schools can only get 90 percent of their money from the Federal Government. The other 10 percent has to come from someplace else—private sources. But that doesn't count military. If a for-profit school bumps up on the 90–10 level, it cannot go out and recruit any more people, but if it recruits one military person, it can get nine more nonmilitary. So that pays for them to go after the military. Well, Senators CARPER and DURBIN have a bill in to stop that.

Senator DURBIN is also a leader on the issue of private student loans and bankruptcy, as well as a great partner in helping to draw attention to the experiences of students who have attended these schools.

I also thank other members of the HELP Committee who have been active participants at hearings, including Senators FRANKEN, MERKLEY, and BLUMENTHAL.

I have also received a great deal of support and encouragement along the way from organizations dedicated to ensuring that students have a genuine path to success in higher education. In particular, I thank the Council for Opportunity in Education, the Education Trust, the Leadership Council on Civil Rights, the Institute for College Access

and Success, Campus Progress, and the National Association for College Admissions Counseling. All of them have been involved in helping us over the last couple of years to get the data we needed.

On behalf of servicemembers and veterans, we have had tremendous assistance from the Iraq and Afghanistan Veterans Association, the Veterans of Foreign Wars, the Military Officers Association of America, Blue Star Families, the Vietnam Veterans Association, Student Veterans of America, the American Legion, VetJobs, VetsFirst, Paralyzed Veterans of America, the National Association for Black Veterans, the National Guard Association, the Air Force Sergeants Association, the Association of the United States Navy, Wounded Warriors, and Veterans for Common Sense. All of them have been involved. We have gone to them, and they have been so forthcoming and helpful, helping our staff and me to understand what is happening.

I also thank the witnesses at our hearings, several of whom have been subjected to unwarranted and undeserved criticism. In particular, I thank Steve Eisman, who provided the committee with unique expertise and insights about the industry in a way that helped policymakers understand that these companies were much more than just colleges. As everyone in this body knows, people with a financial stake in an industry testify before Congress every day and, like Mr. Eisman, provide some of the most insightful and accurate information we receive.

I also thank former Westwood employee Joshua Pruyn, who provided a real-world view of working as a for-profit recruiter. He was willing to come forward for the sole purpose of shedding light on this industry, and the criticism he has sustained speaks poorly of those who claim to believe in the valuable role whistleblowers play.

I thank my staff, who have pursued this investigation tirelessly and tenaciously.

I thank my oversight team and my HELP Committee, who spearheaded the investigation, analyzed the numbers, calculated all of the outcomes, interviewed students and employees, reviewed thousands of pages of documents, and prepared this final report. That oversight team was led by Beth Stein. She was assisted throughout six hearings, three previous reports, many spreadsheets, charts, and megabytes of documents by Elizabeth Baylor and Ryan McCord. More recently, they were joined by Kia Hamadanchy and Bryan Boroughs, who have dedicated many long hours to the research, writing, and publication of this report.

I also owe a tremendous thanks to several staffers who are no longer with the committee but played a critical role in this investigation: Beth Little, Luke Swarthout, and Robin Juliano.

I also thank my former and current HELP Committee staff directors, Dan Smith and Pam Smith, who have ably guided this sometimes challenging effort.

Our communications staffers have patiently explained the 90–10 rule, the cohort default rate, and the fact that we don't actually know how veterans attending for-profit schools are doing to hundreds of reporters throughout the country. I thank Justine Sessions, Kate Frischmann, and Liz Donovan.

I also thank my education policy staffers who joined this effort more recently but who will be carrying us forward in our legislative reform efforts: Mildred Otero, Spiros Protopsaltis, and Libby Masiuk, as well as Carrie Wofford, who has played a tremendous role in outreach to groups across the country and has been a particular advocate on behalf of veterans impacted by the practices of the for-profit colleges.

I also thank our tremendous group of law clerks, who dedicated many hours to the less glamorous tasks of getting this put together: Abre Connor, Joel Murray, Lauren Scott, David Krem, Ashley Waddell, Lindsey Daughtry, Zach Mason, Sophie Kasimow, and Brittany Clement.

A special thank-you goes to the law clerks who helped write and prepare the report: Lucy Stein, Nicholas Wunder, Shauna Agean, Keagan Buchanan, and Douglas Dorando, and also Andrea Jarcho, who has juggled multiple roles and worn multiple hats.

For their assistance along the way, I also thank Paul Edenfield, Madeline Daniels, Alyssa Davis, and also Dan Goldberg for his always-sound analysis and advice.

Finally, I thank Denise Lowrey and Carolyn Bolden, on the committee staff, who spent many hours making the report as error-free as humanly possible.

Today we bring the HELP Committee investigation of for-profit colleges to a close, but the record we have laid out leaves much to be done, and I look forward to continuing to work with my Senate colleagues to help for-profit colleges realize their potential as a genuinely transformative force in higher education.

With that, I yield the floor.

The ACTING PRESIDENT pro tempore. The Senator from Vermont.

GLOBAL WARMING

Mr. SANDERS. Mr. President, the Senator from Oklahoma, JIM INHOFE, is a friend of mine. While we have strong philosophical and political differences, we have had a very positive personal relationship since I entered the Senate 5½ years ago. I like Senator INHOFE, and on occasion, despite our political differences, we have been able to work together as members of the Environment and Public Works Committee, on which we both sit. I especially applaud the Senator for his strong efforts on the recently passed Transportation bill in which he led the effort in getting his fellow Republicans to move forward on the vitally important issue of rebuilding our crumbling infrastructure—in this case, roads and bridges.

Unfortunately, Senator INHOFE has some very radical views regarding global warming. I believe he is dead wrong and dangerously wrong on this issue. Not only is he wrong, but because he is the leading Republican on the Environment Committee, his views hold great influence over other Republicans in the Senate, in the House, and across the country. Because many Republicans follow Senator INHOFE's lead, it means we are making very little progress in Congress in combating what most of the scientific community sees is a global environmental crisis.

I am on the floor today to ask Senator INHOFE to rethink his views on this enormously important issue and to ask my Republican colleagues to do the same. I am asking them to join the overwhelming majority of scientists who have studied and written about this issue in understanding that, one, global warming is real; two, global warming is significantly caused by human activity; three, global warming is already causing massive and costly destruction to the United States and around the world, and it will only get worse in years to come.

I am also asking Senator INHOFE and my Republican colleagues to understand that the United States, with all of our knowledge, all of our expertise, and all of our technology, can and must lead the rest of the world, which must follow our effort in cutting back on carbon emissions and reverse global warming, and to understand that when we do this—when we transform our energy system away from fossil fuels and enter into energy efficiency and sustainable energy—when we do that over a period of years, we can create millions of good-paying jobs.

What I want to do this afternoon is nothing more than to simply quote some of the statements and assertions Senator INHOFE has made and to express to you why he is dead wrong and dangerously wrong on this vitally important issue.

Mr. President, on July 11—just 2½ weeks ago—Senator INHOFE spoke on this floor reiterating his longstanding views on global warming. What he said during that speech is pretty much what he has been saying for years. I read that speech, and I want to use this opportunity to comment on it. Specifically, I want to discuss a number of observations in which Senator INHOFE is completely wrong.

First and foremost, Senator INHOFE tells us in his speech that global warming science is wrong. First and foremost, Senator INHOFE tells us in his speech that global warming science is wrong. Mr. INHOFE states, on page S4860 of the CONGRESSIONAL RECORD from July 11—and I will do my best to quote him as accurately as I possibly can—the following about global warming:

> In 2003 . . . I started hearing from a lot of the real scientists that it was a hoax.

And Senator INHOFE continued, again from July 11, 2012:

> It is the greatest hoax ever perpetrated on the American people.

Let me repeat again what Senator INHOFE said just a few weeks ago on the floor of the U.S. Senate.

[Global warming] . . . is the greatest hoax ever perpetrated on the American people.

In fact, the title of Senator INHOFE's new book—which he was kind enough to give me a copy of—is ''The Greatest Hoax.'' That is the title of his book.

Well, let's examine that assertion on the part of Senator INHOFE. The United States Global Change Research Program, which was supported and expanded by President George W. Bush, a conservative Republican, and which includes scientists at NASA, EPA, the Department of Defense, the Department of Agriculture, the Department of Energy, the State Department, the Department of Health, the Departments of Transportation, Commerce, and Interior, have said:

Global warming is unequivocal and primarily human-induced.

Senator INHOFE has said global warming is a hoax, but the Global Change Research Program, which brings together many departments of the U.S. Government, says:

Global warming is unequivocal and primarily human-induced.

Our National Academy of Sciences joined with academies in Brazil, Canada, China, France, Germany, India, Italy, Japan, Mexico, Russia, South Africa, and the United Kingdom. They all came together and said:

The need for urgent action to address climate change is now indisputable.

It is now indisputable. Senator INHOFE says global warming is a hoax; academies of science all over the world state the need for urgent action to address climate change is now indisputable.

Eighteen scientific professional societies, including the American Geophysical Union, the American Chemical Society, and others say:

Climate change is occurring and rigorous scientific research demonstrates that the greenhouse gases emitted by human activities are the primary driver.

That is a quote from 18 scientific professional societies. Senator INHOFE says global warming is a hoax, but 18 scientific professional societies say climate change is occurring and rigorous scientific research demonstrates that the greenhouse gases emitted by human activities are the primary driver.

Even noted climate skeptic Richard Muller, who, interestingly enough, Senator INHOFE has cited in his own speeches over the years, wrote in the Wall Street Journal last year that his latest research proved ''global warming is real.'' More to the point, in an op-ed published 2 days ago, Richard Muller, who in the past was cited by Senator INHOFE as a global warming skeptic, wrote an op-ed in the New York Times entitled ''The Conversion of a Climate Change Skeptic.''

Mr. President, I ask unanimous consent to have printed in the RECORD the op-ed I have just referred to.

The ACTING PRESIDENT pro tempore. Without objection, it is so ordered.

(See exhibit 1.)

Mr. SANDERS. Mr. President, this is how Richard A. Muller—again, the scientist who was often quoted by Senator INHOFE—began his op-ed 2 days ago in the New York Times. This is the quote from Richard A. Muller.

Call me a converted skeptic. Three years ago, I identified problems in previous climate studies that, in my mind, threw doubt on the very existence of global warming. Last year, following an intensive research effort involving a dozen scientists, I concluded that global warming was real and that the prior estimates of the rate of warming were correct. I'm now going a step further: Humans are almost entirely the cause.

And Dr. Muller continues:

My total turnaround, in such a short time, is the result of careful and objective analysis by the Berkeley Earth Surface Temperature project, which I founded with my daughter Elizabeth. Our results show that the average temperature of the earth's land has risen by 2½ degrees Fahrenheit over the past 250 years, including an increase of 1½ degrees over the most recent 50 years. Moreover, it appears likely that essentially all of this increase results from the human emission of greenhouse gases.

That was Dr. Richard Muller from an op-ed in the New York Times on July 28, 2012.

I am not going to tell you that every single serious scientist in the world agrees with Dr. Muller or agrees with me or agrees with the vast majority of scientists that global warming is real and primarily caused by human activity. But I will say that, according to the National Academy of Sciences, approximately 98 percent of active climate scientists who published peer-reviewed papers agree with the assertion that global warming is occurring and human activity is a significant driver of it—not 100 percent but 98 percent.

When we talk about scientists publishing with peer review, what we are saying is their papers and research were reviewed and examined by other expert scientists in their field. That is the great thing about science and peer review. The process invites criticism and invites other scientists to prove your idea is wrong. When we say 98 percent of active climate scientists agree about global warming, we are talking about scientists whose work has been examined critically and found to be well-documented and correct by their peers in the field.

This is an important point to be made. There may well be scientists out there who may have different views. But by and large they have not written peer-reviewed literature which has been examined by other experts in that field. So the bottom line here—and the important bottom line—is when Senator JIM INHOFE says global warming is a hoax, he is dead wrong according to the overwhelming majority of scientists who have studied this issue.

I hope very much—and I mean this sincerely, because this is an enormously important issue—that Senator INHOFE will rethink his position, and those Republicans who have followed Senator INHOFE's lead will also rethink their position.

In July of 2010, in an interview with ABC News, Senator INHOFE said:

We're in a cycle now that all the scientists agree is going into a cooling period.

Let me repeat that, because I don't want anyone to think I made a mistake about what I said. July 2010, ABC News, quoting Senator INHOFE.

We're in a cycle now that all the scientists agree is going into a cooling period.

On July 11, on the floor of the Senate, Senator INHOFE stated in his remarks—and this is found on page S4860 of the CONGRESSIONAL RECORD. I want everyone to make sure I am not misquoting Senator INHOFE. I would not do that. From page S4860 of July 11, the CONGRESSIONAL RECORD:

. . . we went into a warming period that went up to the turn of the century. Now it is actually going down into a cooling period again . . .

That was Senator INHOFE, July 11, 2012. In other words, as I understand it, Senator INHOFE is saying that since the year 2001 we are in a cooling period. Unfortunately, Senator INHOFE's assertion that we have entered a cooling period could not be more incorrect.

Let's look at what the scientific data shows us. The last decade was not one where our temperature got cooler. It was, in fact, the very opposite. According to NASA, the last decade was in fact the warmest on record, using temperature records that date to the late 1800s. NASA's data shows that 9 of the 10 warmest years on record occurred since 2000, when Senator INHOFE says we went into a ''cooling period.'' So NASA says the last decade was the warmest on record, but Senator INHOFE says we have gone into a cooling period.

But it is not just NASA making this finding. The National Oceanic and Atmospheric Administration—NOAA—issued a report from 300 scientists in 48 countries that confirms the last decade was the warmest on record—the warmest on record at a time when Senator INHOFE tells us we are going into a cooling period.

The World Meteorological Organization also confirms that the last decade was the warmest on record, and they found the 13 warmest years on record have all occurred since 1997.

So the American people and my Republican friends are going to have to make a decision: Is JIM INHOFE right that we are entering into a cooling period or is NASA and the National Oceanic and Atmospheric Administration correct in saying that the last decade was, in fact, the warmest on record?

As my fellow Vermonter, Bill McKibben, recently pointed out, globally we have seen 327 consecutive months where the temperature exceeded the global average for the 20th century. Senator INHOFE tells us the world is getting cooler, but science shows us we have just experienced the warmest

decade on record. Somebody is right and somebody is wrong, and I do not believe Senator INHOFE is right.

Senator INHOFE stated on July 11, 2012, page S. 4862 of the CONGRESSIONAL RECORD:

> One thing we did find out when we got a report from several universities, including MIT, was that the cost of this, if we were to pass any of the bills, would have been between $300 billion and $400 billion a year.

This is not the first time Senator INHOFE has asserted that the cost of cutting greenhouse gas emissions is $300 billion to $400 billion a year. In an interview with Fox News on February 11, 2000, Senator INHOFE was asked by the Fox anchor about the cost of global warming legislation, and he responded:

> It would cost between $300 billion and $400 billion a year.

Senator INHOFE gets his estimates by looking at worst-case scenarios from an out-of-date report that looked at legislation from 2007. The truth is, however, more recent research proves we can take strong action to cut emissions while at the same time growing our economy and saving Americans substantial sums of money on their energy bills.

For example, a 2009 study from McKinsey consulting firm found that the United States can meet our 2020 targets for greenhouse gas emission reductions just through cost-effective energy efficiency efforts, with a net savings for American consumers of $700 billion. A 2010 report from the American Council for an Energy Efficient Economy found that by doing things nationally, many States—including the State of Vermont, my own State—are doing on energy efficiency already, we could achieve substantial benefits. The study found by investing aggressively in energy efficiency in our buildings, in our schools, in our factories, and in our transportation systems we would create over 370,000 net new jobs by 2020, boost our rate of economic growth and GDP, and save households significant sums of money on their energy bills—all while vastly exceeding our 2020 target of cutting greenhouse gas emissions 17 percent from 2005 levels.

In this scenario, we could cut emissions over 30 percent by 2020 as we create jobs and as millions of people save money on their energy bills. To my mind, creating jobs, cutting greenhouse gas emissions, and saving money on people's fuel bills is a win-win-win situation.

In addition to the clear benefits from taking action, I want to point out to Senator INHOFE the costs and risks if we do not take action, if we do nothing. The alternative is we step back, we don't do anything, and what happens?

Already, the extreme weather we have seen is impacting our Nation's infrastructure. An interesting article appeared just a few days ago, July 25, 2012, in the New York Times. It said the Nation's infrastructure is being taxed to worrisome degrees by heat, drought, and vicious storms. The article noted that on a single day in July, an airplane got stuck in asphalt that softened due to 100-degree temperatures, and a subway train derailed after heat caused a track to bend. It also cited highways that are heating up and expanding beyond their design limits, causing cracks and jarring bumps in the road. The article mentioned how powerplants are having difficulty using their regular cooling sources during operation because the water is now excessively warm.

A power company executive with 38 years of experience was quoted as saying:

> We've got the storm of the century every year now, after power was knocked out for 4.3 million people in 10 States after the June derecho storm that raced from the Midwest to the East Coast at near hurricane-force winds.

Interestingly, not generally noted as being terribly progressive, the insurance industry has noted their costs for property damage from increasingly extreme weather have already increased in the United States from $3 billion a year in the 1980s to $20 billion a year today. According to Mark Way, an official with Swiss Re, a large reinsurance company:

> A warming climate will only add to this trend of increasing losses, which is why action is needed now.

A landmark study prepared for the British Government by Nicholas Stern, former chief economist of the World Bank, found that doing nothing to reverse global warming could eventually shrink the global economy by 20 percent. The Chairman of the National Intelligence Council under President George W. Bush testified to Congress that intelligence assessments indicated that global warming could worsen existing problems, such as poverty, social tensions, environmental degradation, ineffectual leadership, and weak political institutions. Climate change could threaten domestic stability in some States, potentially contributing to conflict, particularly over access to increasingly scarce water resources.

Unlike Senator INHOFE, most Americans are seeing the evidence of global warming with their own eyes. I want to take some time to talk about what we are seeing.

The Associated Press reported on July 3, 2012:

> But since at least 1988, climate scientists have warned that climate change would bring, in general, increased heat waves, more droughts, more sudden downpours, more widespread wildfires and worsening storms. In the United States, those extremes are happening here and now.
>
> So far this year, more than 2.1 million acres have burned in wildfires, more than 113 million people in the U.S. were in areas under extreme heat advisories last Friday, two-thirds of the country is experiencing drought, and earlier in June, deluges flooded Minnesota and Florida.

We saw extreme weather last year as well. In 2011, we had a record-breaking 14 weather disasters in the United States that each caused over $1 billion in damage. One of those was Hurricane Irene, which caused devastating flooding and loss of life in the State of Vermont and other States in the Northeast and Mid-Atlantic. According to FEMA:

> Considered together, the federally declared disasters of 2011 presented crises all but unprecedented in their frequency and scope. The 99 major disasters, 29 declared emergencies, and 114 requests for fire management assistance touched 48 out of 50 states.

In other words, 48 States had a federally declared disaster last year.

Global average surface temperature has already increased 1.3 degrees Fahrenheit since 1900, according to NOAA. The last 12 months is the warmest 12-month period on record in the United States. Since January 1, 2012, cities and regions in the United States have set 40,000 records for warm temperatures, compared to just 6,000 for cold temperatures, according to NOAA. In the 20th century we set warm and cold temperature records at roughly a 1-to-1 ratio. In the 21st century, that has changed 2 to 1 in favor of heat records, and this year it has jumped to 7 to 1.

As the planet warms, we are seeing more extreme heat wave events. Heat waves killed tens of thousands in Europe in 2003 and Russia in 2010, and a heat wave in Texas and Oklahoma caused severe drought and wildfires in 2011. Global warming made these heat waves significantly more likely, according to the latest science.

Leading climatologist James Hansen and several of his colleagues published a report that said:

> Extreme heat waves such as that in Texas and Oklahoma in 2011, and Moscow in 2010, were caused by global warming, because their likelihood was negligible prior to the recent rapid global warming.

Another study from German researchers published in the U.S. National Academy of Sciences found an 80-percent likelihood that the Russian heat wave in 2010 was attributable to global warming. And a study from NOAA found the heat wave and drought in Texas in 2011 was 20 times more likely to occur today than 50 years ago due to the warming of the planet.

As I mentioned, this country is currently experiencing a devastating drought. The U.S. Department of Agriculture has designated disaster areas due to drought in 1,369 counties in 31 States this year. The price of corn has increased 50 percent in the last 3 months, and soybean prices are up 25 percent since June. This is because 78 percent of the corn crop and 77 percent of soybean production is in drought-affected areas.

This is not the first time we have seen devastating droughts spike food prices in recent years. Severe drought in Russia in 2010 led that country to ban exports of grain, which contributed to a near doubling in wheat prices over a 2-month period in that year. The worst drought in China in 60 years occurred last year in 2011, affecting 12 million acres of wheat and contributing—along with floods in Australia

and the drought in Russia—to record food prices.

Some commentators cited the record food prices caused by these extreme weather events as contributing to unrest. When food prices go up, there is often instability in countries around the world—including the Middle East and Africa.

Sea levels have already risen 7 inches globally, according to EPA. We have seen during the last three summers record low levels of Arctic Sea ice, and we know from NASA satellites that Antarctica is losing 24 cubic miles of ice every year. In Glacier National Park in this country we had 150 glaciers when it was formed in 1910, but today only 25 remain. Some studies predict a sea level rise of 5 feet or more by the end of this century. But even if sea levels rose 3 feet, cities such as Miami, New Orleans, Charleston, SC, Oakland, CA, and others could find themselves partially underwater.

The average annual acreage consumed by wildfires in the United States more than doubled during the last decade compared with the previous four decades. Last year in Texas wildfires destroyed 2,700 homes. This year in Colorado—the most destructive wildfire in that State's history—destroyed 350 homes. Wildfires in Colorado this year caused tens of thousands to evacuate their homes. In New Mexico, we saw the largest wildfire in that State's history this year burn more than 170,000 acres that broke the previous record which was set just last year when a fire burned more than 150,000 acres.

Mr. President, last year floods along the Mississippi River caused $2 billion worth of damage. Floods in North Dakota displaced 11,000 people from their homes. Record floods in Australia in 2011 caused its State of Queensland to conduct the largest evacuation in its history. Floods in Pakistan in 2010 killed 2,000 people and left one-fifth of that nuclear-armed nation under water for weeks. That is the kind of potentially destabilizing extreme weather events the folks at the Department of Defense and the CIA worry about. Unfortunately, I could go on and on. The bad news is if we do nothing, the science is clear that temperatures will continue to increase, sea levels will continue to rise, and extreme weather will become more frequent and more devastating. The good news is—and it is very good news—that we now have the technology, the knowledge, and the know-how to cut emissions today through energy efficiency and through moving toward such sustainable and renewable technologies as solar, wind, geothermal, and biomass.

It is time for Congress to get serious about global warming and to work to transform our energy system to sustainable energy, and that starts by beginning to understand that global warming is real and that if we do not address it now, it will only get worse and bring more danger to this country and to our planet.

Mr. INHOFE. Will the Senator yield for a unanimous consent request?

Mr. SANDERS. Yes.

Mr. INHOFE. Mr. President, I ask unanimous consent that at the conclusion of the remarks of my friend from Vermont, I be recognized as in morning business for such time as I will consume.

The ACTING PRESIDENT pro tempore. Is there objection?

Without objection, it is so ordered.

Mr. SANDERS. Mr. President, I am glad to see my friend from Oklahoma here on the floor. I want to conclude by reading a review of Senator INHOFE's book, which is called ''The Greatest Hoax,'' by a gentleman named J.C. Moore. This review by J.C. Moore was published in the Tulsa World which is, I suspect, the largest newspaper in the State of Oklahoma. J.C. Moore is a native Oklahoman—the same State Senator INHOFE represents—and a Ph.D. who taught chemistry and physics and is a member of the American Geophysical Union.

This is what Mr. Moore wrote: ''Inhofe claims he is winning in his fight to debunk global warming.'' After discussing the scientific consensus among climate scientists and major scientific institutions all over the world, Moore writes:

> Inhofe's greatest adversary is nature itself, as research shows the climate is changing in response to human activities. The amount of carbon dioxide in the atmosphere is increasing, the temperature of the Earth is rising, the oceans are becoming more acidic, glaciers and polar ice caps are melting, sea levels are rising, the probability of severe weather events is increasing, and weather-related natural disasters are becoming more frequent and more costly. It is time we examine more closely who is actually winning by ignoring science.

As I understand it, that is from a review of Senator INHOFE's book, ''The Greatest Hoax,'' by a gentleman named J.C. Moore in the Tulsa World.

There is much more to be said on this issue because here on the floor of the Senate we are saying virtually nothing. I might say that we look pretty dumb to the rest of the world by ignoring what many scientists believe is the major environmental crisis of our time which, if we don't get a handle on, will have profound impacts on the well-being of this country and countries throughout this world.

So I say to my friend Senator INHOFE—and he is my friend—I hope very much the Senator will rethink his position. I hope those Republicans who are following the Senator's lead will rethink their position because nothing less than the future of our planet is at stake.

EXHIBIT 1

[From the New York Times, July 28, 2012]

THE CONVERSION OF A CLIMATE-CHANGE SKEPTIC

(By Richard A. Muller)

Call me a converted skeptic. Three years ago I identified problems in previous climate studies that, in my mind, threw doubt on the very existence of global warming. Last year, following an intensive research effort involving a dozen scientists, I concluded that global warming was real and that the prior estimates of the rate of warming were correct. I'm now going a step further: Humans are almost entirely the cause.

My total turnaround, in such a short time, is the result of careful and objective analysis by the Berkeley Earth Surface Temperature project, which I founded with my daughter Elizabeth. Our results show that the average temperature of the earth's land has risen by two and a half degrees Fahrenheit over the past 250 years, including an increase of one and a half degrees over the most recent 50 years. Moreover, it appears likely that essentially all of this increase results from the human emission of greenhouse gases.

These findings are stronger than those of the Intergovernmental Panel on Climate Change, the United Nations group that defines the scientific and diplomatic consensus on global warming. In its 2007 report, the I.P.C.C. concluded only that most of the warming of the prior 50 years could be attributed to humans. It was possible, according to the I.P.C.C. consensus statement, that the warming before 1956 could be because of changes in solar activity, and that even a substantial part of the more recent warming could be natural.

Our Berkeley Earth approach used sophisticated statistical methods developed largely by our lead scientist, Robert Rohde, which allowed us to determine earth land temperature much further back in time. We carefully studied issues raised by skeptics: biases from urban heating (we duplicated our results using rural data alone), from data selection (prior groups selected fewer than 20 percent of the available temperature stations; we used virtually 100 percent), from poor station quality (we separately analyzed good stations and poor ones) and from human intervention and data adjustment (our work is completely automated and hands-off). In our papers we demonstrate that none of these potentially troublesome effects unduly biased our conclusions.

The historic temperature pattern we observed has abrupt dips that match the emissions of known explosive volcanic eruptions; the particulates from such events reflect sunlight, make for beautiful sunsets and cool the earth's surface for a few years. There are small, rapid variations attributable to El Niño and other ocean currents such as the Gulf Stream; because of such oscillations, the ''flattening'' of the recent temperature rise that some people claim is not, in our view, statistically significant. What has caused the gradual but systematic rise of two and a half degrees? We tried fitting the shape to simple math functions (exponentials, polynomials), to solar activity and even to rising functions like world population. By far the best match was to the record of atmospheric carbon dioxide, measured from atmospheric samples and air trapped in polar ice.

Just as important, our record is long enough that we could search for the fingerprint of solar variability, based on the historical record of sunspots. That fingerprint is absent. Although the I.P.C.C. allowed for the possibility that variations in sunlight could have ended the ''Little Ice Age,'' a period of cooling from the 14th century to about 1850, our data argues strongly that the temperature rise of the past 250 years cannot be attributed to solar changes. This conclusion is, in retrospect, not too surprising; we've learned from satellite measurements that solar activity changes the brightness of the sun very little.

How definite is the attribution to humans? The carbon dioxide curve gives a better match than anything else we've tried. Its

magnitude is consistent with the calculated greenhouse effect—fextra warming from trapped heat radiation. These facts don't prove causality and they shouldn't end skepticism, but they raise the bar: to be considered seriously, an alternative explanation must match the data at least as well as carbon dioxide does. Adding methane, a second greenhouse gas, to our analysis doesn't change the results. Moreover, our analysis does not depend on large, complex global climate models, the huge computer programs that are notorious for their hidden assumptions and adjustable parameters. Our result is based simply on the close agreement between the shape of the observed temperature rise and the known greenhouse gas increase.

It's a scientist's duty to be properly skeptical. I still find that much, if not most, of what is attributed to climate change is speculative, exaggerated or just plain wrong. I've analyzed some of the most alarmist claims, and my skepticism about them hasn't changed.

Hurricane Katrina cannot be attributed to global warming. The number of hurricanes hitting the United States has been going down, not up; likewise for intense tornadoes. Polar bears aren't dying from receding ice, and the Himalayan glaciers aren't going to melt by 2035. And it's possible that we are currently no warmer than we were a thousand years ago, during the ''Medieval Warm Period'' or ''Medieval Optimum,'' an interval of warm conditions known from historical records and indirect evidence like tree rings. And the recent warm spell in the United States happens to be more than offset by cooling elsewhere in the world, so its link to ''global'' warming is weaker than tenuous.

The careful analysis by our team is laid out in five scientific papers now online at BerkeleyEarth.org. That site also shows our chart of temperature from 1753 to the present, with its clear fingerprint of volcanoes and carbon dioxide, but containing no component that matches solar activity. Four of our papers have undergone extensive scrutiny by the scientific community, and the newest, a paper with the analysis of the human component, is now posted, along with the data and computer programs used. Such transparency is the heart of the scientific method; if you find our conclusions implausible, tell us of any errors of data or analysis.

What about the future? As carbon dioxide emissions increase, the temperature should continue to rise. I expect the rate of warming to proceed at a steady pace, about one and a half degrees over land in the next 50 years, less if the oceans are included. But if China continues its rapid economic growth (it has averaged 10 percent per year over the last 20 years) and its vast use of coal (it typically adds one new gigawatt per month), then that same warming could take place in less than 20 years.

Science is that narrow realm of knowledge that, in principle, is universally accepted. I embarked on this analysis to answer questions that, to my mind, had not been answered. I hope that the Berkeley Earth analysis will help settle the scientific debate regarding global warming and its human causes. Then comes the difficult part: agreeing across the political and diplomatic spectrum about what can and should be done.

With that, I am happy to yield the floor for my friend, Senator INHOFE of Oklahoma.

The ACTING PRESIDENT pro tempore. The Senator from Oklahoma.

Mr. INHOFE. Mr. President, first of all, something my friend from Vermont said a minute ago would surprise a lot of people, and that is we are friends. It is kind of strange. People don't understand being violently opposed to each other in this body and yet also being very close friends. My friend from Vermont has a different philosophy than I do. That is the nice thing about both the House and the Senate. We have people with different philosophies who believe in different things. Somewhere in the midst of this, the truth ultimately does come out most of the time. I think we would probably agree with that.

One thing I like about my friend from Vermont is he really believes and is willing to stand up and fight for something he believes. I am not going to suggest there are hypocrites in this body. I wouldn't say that at all. When we look around the political scene, we see people who somehow might ingratiate a block of people who are wanting support. Maybe it is for the next election, maybe it is for a cause. That is not the case with my friend from Vermont. He believes in his heart everything he says.

Sometimes I talk to young people who come in as interns. I tell them there are varied philosophies in the Senate and in the House. We have extreme liberals who believe our country should have a greater involvement in the decisions we make. We have conservatives, like I am, who believe we have too much government in our lives as it is. It is a basic difference. But I say to them, even though I am on the conservative side, I would rather someone be a far outspoken liberal extremist than be in the mushy middle and not stand for anything. My friend from Vermont is not in the mushy middle. He stands for something.

It was not too long ago that another friend in his office, his press secretary—we are very close friends—said something, and I don't want to misquote him. He said, My boss would like to have a copy of your book. I said, Not only will I give him a copy, but I will autograph it for him, but with one commitment, and that is he has to read it. He kept that commitment; I can tell by the things he said.

Let me go over a few things that were said, and I think it is interesting. This Dr. Richard Muller—I can't recall too much about him, but I do know he was listed among scientists who were skeptics. For the benefit of people who may not know the terminology, I refer to an alarmist as someone who thinks there is great alarm because something is happening and the end of the world is coming because of global warming. Skeptics are those like myself who don't believe that. He apparently has changed from being a skeptic to an alarmist. I would only say this, and that is my Web site, epw.senate.gov, shows from probably over 12 years ago a list of scientists who are calling me, making statements, and saying that the IPCC—that is the United Nations, and that is what we are talking about. The United Nations came out with a preconceived notion that they wanted to believe a preconceived conclusion. When they did this, the scientists who were included in the process were scientists who agreed with them.

So when I questioned it by standing on the floor—I don't remember the date of this. My friend from Vermont may remember that. I made statements about two or three scientists who had called me. After that, the phone was ringing off the hook. Keep in mind there are a lot of scientists out there. We listed on the Web site up to over 1,000 scientists who declared they were skeptics about this whole thing. So I can take some gratitude about the fact that the only scientist who was on the skeptic list who has changed to an alarmist is 1 out of 1,000.

My friend was talking about the National Academy of Sciences. I think it is kind of interesting because let's remember it was the National Academy of Sciences that came out with a report in 1975 warning of a coming ice age. Keep in mind we are all going to die whether it is global warming or another ice age. That is the National Academy of Sciences, the same group. According to a lot of people, they have turned themselves into an advocacy group.

I will quote MIT's Dr. Richard Lindzen, who was a former U.N. IPCC reviewer. He was talking about Ralph Cicerone, who is the president of the NAS. He said:

> Cicerone of NAS is saying that regardless of evidence the answer is predetermined, if gov't wants carbon control, that is the answer—

That is what the NAS will provide. If you control carbon, you control life.

So we have had a lot of differing and varying interpretations of availing science over the years. I can recall one of my first introductions to this. Of course, this came way back during the Kyoto Convention. Some people have forgotten that Kyoto was a convention that was going to get everyone to get together under the leadership of the United Nations and we were all going to reduce our carbon, and so they had this big meeting down there. I will always remember it. This is the famous Al Gore meeting that was called the Earth Summit of 1992. So they came out with this and said this is going to happen. The United Nations said it is, and so they thought everything was fine. Everyone believed it.

It was shortly after that I remember hearing someone talk about it. We can go back and look at this. This is not something I am just saying. There were statements that were made in the 30-year period—let's take the 30-year period from 1895 to 1925. That is 30 years. During that time everyone feared that another ice age was coming. They talked about another ice age, and that the world was coming to an end. They provided all of this documentation during that 30-year period that that is what was happening.

Well, from 1925 to 1945, that 20-year period was a global warming. In fact,

the first time we heard of global warming was in that 20-year period from 1925 to 1945. So the world was going to come to an end again, and it was going to be during that period of time due to global warming.

Then came the 30-year period from 1945 to 1975. During that time they said it is a cold spell, and that is when all of these companies came in—the Senator from Vermont is right. I have given probably 30 talks well in excess of an hour each talking about these things. During that time, I remember holding up the cover of Time magazine where they talked about how another ice age was coming. Then I held up a cover of the Time magazine 20 years later, and they said, no, it is global warming. They had the last polar bear stepping on the last cube of ice, and saying we are going to die.

We went through a period of 1945 to 1975 where they declared it a period of another ice age. Then 1975 to the turn of the century—so that was another 30-year period of time—when it was global warming. So we have gone back and forth.

Here is the interesting thing about that. The assertion is always made that we are having catastrophic global warming because of manmade gases, CO_2, anthropogenic gases, and methane. Yet the greatest surge of CO_2 came right after World War II starting in 1945, and that precipitated not a warming period but a cooling period. So when you look at these things, sometimes—by the way, the only disagreement I would have with my friend from Vermont is that he has quoted me as saying some things.

Actually, unlike Al Gore and some of these other people, I recognize I am not an expert. I am not a scientist, but I read what the scientists say. I get my phone calls, I look at it, and I try to apply logic to it and come to my conclusions. So that is what has been happening over the last—oh, it has been now 12 years, I guess, since all this started.

I wish to mention a couple of other things that were said. For example, on the idea of the science—here it is, right here. As far as scientists are concerned, I can remember quoting from the Harvard-Smithsonian study. The study examined results of more than 240 peer-reviewed—''peer-reviewed'' is the term used by my friend from Vermont—the Harvard-Smithsonian study examined the results of more than 240 peer-reviewed papers published by thousands of researchers over the past four decades. The study covers a multitude of geophysical and biological climate indicators. They came to the conclusion that ''climate change is not real. The science is not accurate.''

Then we have another quote from a former President of the National Academy of Sciences. He is Dr. Fred Seitz. He said:

> There is no convincing scientific evidence that human release of carbon dioxide, methane, or other greenhouse gases is causing or will in the foreseeable future cause catastrophic heating of the Earth's atmosphere and disruption of the Earth's climate.

Again, he is a former President of the National Academy of Sciences.

Then we had a study from not long ago done by George Mason University. This is one my friend from Vermont may not have seen. It was called to my attention, and I missed it somehow in the media. It was a survey of 430 weather forecasters by the university, and it found that only 19 percent of the weather forecasters believed that the climate is changing and if so, that it is due to manmade gases—only 19 percent. That means 81 percent of them think it is not.

Dr. Robert Laughlin is a Nobel Prize winner and a Stanford University physicist. He said—this is kind of good. I enjoyed this one. He said:

> Please remain calm: The earth will heal itself. Climate is beyond our power to control. The earth doesn't care about governments or their legislation. Climate change is a matter of geologic time, something that the earth routinely does on its own without asking anyone's permission or explaining itself.

It is happening. I think it is kind of arrogant for people to think we can change this. I am recalling one of the statements made by my good friend that we have all of these—we must provide the leadership.

We have watched these great big annual parties the United Nations has in these exotic places around the world. I can remember going to a few of them. I remember one of them in Milan, Italy. It would have been 2003. I went there. They had ''wanted'' posters on all the telephone polls with my picture and quoted me when I first came out with the hoax statement. These big parties are kind of interesting. I have only gone to three of them, but they have people invited from all over the world. The only price to pay to come to this is to believe that catastrophic warming is taking place and that it is the fault of bad old man and anthropogenic gases.

Anyway, the last one was an interesting one—not the last one, the most enjoyable one in Copenhagen. At that time—I am going from memory, but I believe President Obama had been there, Secretary Clinton had been there, NANCY PELOSI had been there, and several others. There were five different people—I can't remember the other two—and they were there to assure the other countries—keep in mind, 192 countries—they assured them that we were going to pass some type of cap-and-trade legislation. So I went. Right before I went over, I announced myself as a self-described—I don't mean it in an arrogant way—as a self-proclaimed, one-man truth squad. I went over to tell them the truth, that it wasn't going to happen.

But right before it happened—talk about poetic justice, I say to my friend from Vermont—right before that happened was a hearing we had with the director of the EPA, Lisa Jackson, whom I love dearly. She is one of my three favorite liberals whom I often talk about, and she came out and said—I looked at her and I said: I am going to Copenhagen tomorrow. I have a feeling that when I leave to go to Copenhagen, you are going to have a declaration that will declare that it is a hazard and all this and give the bureaucracy justification to do through regulation what they could not do and have not been successful in doing through legislation.

I saw a smile on her face.

I said: In the event you make that finding, it has to be based on science. What science do you think it will be based on?

She said: Well, primarily the IPCC—the Intergovernmental Panel on Climate Change.

It is a branch of the United Nations. It was all started by the United Nations.

By the way, I would not mention my book; however, I checked before I came down, and if somebody else mentions my book, which is ''The Greatest Hoax,'' then it is all right for me to mention it. I see my friend from Vermont nodding in agreement. So I want people to read the longest chapter, which is the chapter on the United Nations. It goes back and tells what the motives were for this. It goes back to 1972. We were in the midst of an ice age at that time, if my colleague remembers. It talks about the meeting that was going to be held at the Earth Summit in 1992, what the motivation was, and then it goes forward from there.

Here is what is interesting. I was going to mention this in a hearing we will both be attending tomorrow. They had the Earth Summit Plus 20 just a month ago in Rio de Janeiro, the same place it was held 20 years before that when George Bush was President of the United States. He went down there even though he didn't really agree with the stuff that was going on. In this case, President Obama didn't even go down. In fact, it has been conspicuous.

I was glad to see my friend from Vermont coming to the floor and talking about an issue that hasn't been talked about now for years. I am glad it is coming up again. I am glad people realize the cost it is going to be to the American people. By the way, the $300 billion to $400 billion originated from a study that was done by scientists—I am sorry—by economists from the Wharton School, and they came up with that figure. Later on, MIT and several universities said: Well, that is the $300 billion to $400 billion, what it will cost. So that has been pretty much agreed to. Yet I am sure there is a dissenting view. But this is the first time I have heard on the floor of this Senate a denial of that assertion that was made. Everyone knows what it will cost.

I remember the McCain-Lieberman bill when Senator LIEBERMAN said: Yes, it will cost billions of dollars. There is

no question about it. Cap and trade will cost billions of dollars. The question is, What do we gain from it?

Well, that is a pretty good question.

Getting back to Lisa Jackson, I asked the question—this was in a live hearing. I think the Senator from Vermont may have been there; I don't know for sure. It was live on TV.

I said: The assertion has been made that global warming is—that if we pass something, we are going to be able to stop this horrible thing that is going on right now. Let me ask you for the record, live on TV, in a committee hearing, if we were to pass the cap-and-trade bill—I think it was the Markey bill at that time; I am not sure. Cap and trade is cap and trade—pretty much the same. If we were to pass that, would that lower worldwide emissions of CO_2?

She said: No, it wouldn't.

Wait a minute. This is the Obama-appointed director of the Environmental Protection Agency who said: No, it wouldn't, because the problem isn't here. The problem is in other countries.

I don't remember what countries she named—probably China, India, Mexico. It could be other countries; I am not sure. But nonetheless, she said: No, it really wouldn't do that.

So what we are talking about is this tax on the American people of $300 billion to $400 billion. I remember—and I think the Senator from Vermont remembers this also—way back in 1993, during the first of the Clinton-Gore administration, they had the Clinton-Gore tax increase of 1993. That was an increase of marginal rates, the death tax, capital gains, and I believe it was the largest tax increase in three decades at that time. That was a $32 billion tax increase. This would be a tax increase ten times that rate.

I know there are people—their heads swim when they hear these numbers. It doesn't mean anything to them. I will tell my colleagues what I do. In Oklahoma, I get the number of families who file a tax return, and then I do the math every time somebody comes up. In the case of that increase, of the $300 billion to $400 billion, we are talking about a $3,000 tax increase for each family in my State of Oklahoma that files a tax return. So, fine, if they want to do that, they can try to do it, but let's not say something good will come from it when the director of the EPA herself said no, it is not going to reduce emissions.

The other thing too that my friend from Vermont mentioned was the heat. Yes, it is hot. In fact, it was kind of funny—during the remarks of my friend from Vermont, my wife called me from Oklahoma and said: Do you think I should call in and say today it is 109 degrees?

I said: No, it wouldn't be a good idea. Let me say it.

So it is true. Now and then we have some very hot summers, and in the case of my State of Oklahoma, it is hot almost every summer. We have had a lot of heat. However, the people who try to say there is proof that global warming is taking place are the same ones who—back when we had the most severe winter 2 years ago, when my kids built the famous igloo, that was one of the most severe winters. In fact, all the airports were closed at that time. It was kind of funny. I have 20 kids and grandkids. One family is headed up by Jimmy and Molly Rapert. She is a professor at the University of Arkansas. She has a little girl we helped find in Ethiopia many years ago. Zagita Marie was just a few days old when we found her and not in very good shape. We nursed her back to health. Molly and her husband, who have three boys, decided they wanted a girl, and they adopted her. She is now 12 years old. She reads at college level. Every year I have the Africa dinner in February, and she has been the keynote speaker at that.

Anyway, 2 years ago in February, she had given her keynote speech and they were getting ready to leave and go back home, but they couldn't get out because all the airports were closed. What do you do with a family of six? You go out and build an igloo. This wasn't just an igloo the kids built; it slept four people, right next to the Library of Congress, and on top of it they had a little sign saying ''Al Gore's New Home.''

Anyway, they were talking about that single weather event at that time—or some were; not me; I know better than to do that—saying global warming can't take place because we have had the most severe winters. Anyway, a lot of people have tried to use—and I don't blame them for doing it—the idea that, oh, it is really hot out there; therefore, this must be global warming.

I would suggest that—oh, yeah, the one weather event. Roger Pielke, Jr., professor of environmental studies at the University of Colorado, said:

> Over the long run, there is no evidence that disasters are getting worse because of climate change.

Judith Curry, chair of the Georgia Institute of Technology School of Earth and Atmospheric Sciences, said:

> I have been completely unconvinced by any of the arguments that attribute a single extreme weather event or a cluster of extreme weather events or statistics of extreme weather events to an anthropogenic forcing.

Myles Allen, the head of the Climate Dynamics Group at the University of Oxford's Atmospheric, Oceanic and Planetary Physics Department, said:

> When Al Gore said that scientists now have clear proof that climate change is directly responsible for the extreme and devastating floods, storms and droughts, my heart sank.

The other day, I was on the ''Rachel Maddow Show.'' I watch Rachel Maddow. She is one of my three favorite—let me just declare today that I have four favorite liberals, and the Senator from Vermont is one of them. He just graduated to that today, I say to my friend from Vermont.

Anyway, I have been on her show before—and I always like doing it because they are on the other side of these issues—but her own guy, called Bill Nye the Science Guy, agrees, one, it is wrong to try to attribute climate to a weather event. There is a big difference between weather and climate. So we have an awful lot of people who are talking about that.

My good friend from Vermont talked about the global cooling predictions. Let me correct him in saying that I did not say that. I said that quoting scientists. I try to do that because I do not want anyone to think I know that much about science because I do not.

A prominent Russian scientist, Dr. Abdussamatov, said:

> We should fear a deep temperature drop—not catastrophic global warming. . . .
>
> It follows that [global] warming had a natural origin, the contribution of CO_2 to it was insignificant. . . .

This second thing: ''UN Fears (More) Global Cooling Commeth!'' This is the IPCC. This is the United Nations, the same people who, in my opinion—I do say this—are trying to profit from this issue. When I say that, let me clarify that because when the United Nations comes up with something that is not in the best interests of this country—I have often said we ought to correct this. I have written letters, signed by Members of this Senate, and before that by Members of the House when I was in the House, saying: You guys are going to have to come to the meeting and talk about this because it is going to be a serious problem.

When you talk about all these things that are going on, it is something that is not actually taking place.

So they said—and I am quoting now. This would be palaeoclimate scientist Dr. Bob Carter from James Cook University in Australia, who has testified before the U.S. Senate Committee on EPW. I was there at that testimony. He noted on June 18, 2007: The accepted global average temperature statistics used by the Intergovernmental Panel on Climate Change show that no ground-based warming has occurred since 1998. Oddly, this is 8-year long temperature stability that occurred, despite an increase over the same period of 15 parts per million of atmospheric CO_2.

So, again, these are scientists. I know there are scientists with varying views, but there sure are a lot of them here.

Just months before the Copenhagen matter took place—by the way, I kind of enjoyed that trip to Copenhagen because when I got over there—this, again, was the meeting where they invite all the people who believe in global warming and make all these countries—192 countries—believe if they will go along with this, they will get great rewards for doing something about global warming. So, anyway, I enjoyed that very much because I was

able to go over and show the people what the truth was in this country.

But Andrew Revkin, just before Copenhagen, on September 23, 2009, in the New York Times, acknowledged:

> The world leaders who met at the United Nations to discuss climate change . . . are faced with an intricate challenge: building momentum for an international climate treaty at a time when global temperatures have been relatively stable for a decade and may even drop for the next few years.

I look at some of the things—incidentally, I kind of wish I had known my good friend from Vermont was going to be talking about this because I would have been delighted to join in and get a little bit better prepared. But I would say this as to the cost: When you talk about where this cost comes from, the $300 to $400 billion, the Kyoto Protocol and cap-and-trade cost—this is from the Wharton Econometrics Forecasting Associates I mentioned just a minute ago—Kyoto would cost 2.4 million U.S. jobs and reduce GDP by 3.2 percent or about $300 billion annually, an amount greater than the total expenditure on primary and secondary education.

Oh, yes, let's talk about polar bears. I am not sure my friend mentioned the polar bears, so I will skip that part. Anyway, let me just say this: It has become something that has been somewhat of a religion to talk about what is happening and the world is coming to an end. I would just suggest they are not winning that battle.

In March 2010, in a Gallup poll, Americans ranked global warming dead last—8 out of 8—on environmental issues. That was not true 10 years ago. Ten years ago, it was No. 1, and everyone thought that. The more people sit back and look at it and study it, they decide: Well, maybe it is not true after all.

In March 2010, a Rasmussen poll: 72 percent of American voters do not believe global warming is a very serious problem. In a Rasmussen poll at the same time as to the Democrat base: Only 35 percent now think climate change is manmade.

The global warmist Robert Socolow laments:

> We are losing the argument with the general public, big time . . . I think the climate change activists, myself included, have lost the American middle.

In a way, I am kind of pleased it is coming back up and surfacing now. I thank my good friend, and he is my good friend. People do not understand—they really do not understand—what the Senate is all about. The House was not that way when I was in the House. But in the Senate, you can love someone and disagree with them philosophically and come out and talk about it.

I have no doubt in my mind that my friend from Vermont is sincere in what he believes. I believe he would say he knows I am sincere with what I believe. That is what makes this a great body.

But I will just say this: It is popular to say the world is coming to an end. When we look historically, I could go back and talk about what has happened over the years—over the centuries really—and going through these periods of time, and it is always that the world is coming to an end.

Well, I am here to announce—and I feel very good being able to do it with 20 kids and grandkids; I am happy to tell them all right now—the world is not coming to an end, and global warming—we are going through a cycle. We have gone through these cycles before, and every time we go through—in part of my book I talk about the hysterical things people are saying.

Back during that period of time, I mentioned between 1895 and 1930 about how the world was coming to an end, and the same thing from 1930 to the end of the war. Then, of course, getting into the little ice age, all these things that were taking place, the little ice age from 1945—not the ice age but this cooling period—the cooling period that started in 1945 and lasted for 30 years was the time in our history where we had the greatest increase in carbon in the air, the greatest use of that. So it is inconsistent with what reality was.

So I would say to my good friend, I have no doubt in my mind that the Senator from Vermont is sincere in what he says. While he and I are ranked at the extreme sides of the philosophical pendulum, I would say I know he is sincere. But I will also say this is a tough world we are in right now. When we look at the problems we have in this country and the problems we are having in the world and the cost that it has, I am very thankful those who are trying to pass the cap and trade, all the way from the Kyoto Treaty—which was never brought to the Senate, never brought because they knew they were not going to be able to pass it—up until the time when that ended in about 2009, I would say a lot of activists were out there, but I think people have now realized: Just look at the patterns. It gets colder, it gets warmer, it gets colder, it gets warmer. God is still up there. And I think that will continue in the future.

I thank the Chair and yield the remainder of my time.

The PRESIDING OFFICER (Mr. FRANKEN). The Senator from Vermont.

Mr. SANDERS. Mr. President, I have talked for a long time on this issue, so I do not want to make a great speech and continue speaking at great length. I do want to say a few things.

First of all, I want to thank Senator INHOFE for his kind words. Let me respond in the same way. He and I philosophically and politically come from very different places. I have never doubted for one moment the honesty or the sincerity of the Senator from Oklahoma. He is saying what he believes. He has the courage to get up here and say it, and I appreciate that. So we are good friends, and I hope we will continue to be good friends.

I think, frankly, it does this Senate, and it does this country, good when people hear varied differences of opinion on an issue that I consider to be of enormous consequence. So what I would say to my friend is, I hope, in fact, this is the beginning of a resurgence of discussion about this issue, and I look forward to engaging in the discussion with my friend from Oklahoma.

With that, Mr. President, 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.

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

The PRESIDING OFFICER (Mr. WEBB). Without objection, it is so ordered.

EXECUTIVE SESSION

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

The PRESIDING OFFICER. Under the previous order, the Senate will proceed to executive session to consider the following nomination, which the clerk will report.

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

The PRESIDING OFFICER. Under the previous order, there will be 1 hour of debate equally divided and controlled in the usual form.

Mr. LEAHY. Today's debate and vote on the partisan filibuster of the Oklahoma judicial nominee, who has had the support of the Republican Senators from Oklahoma since President Obama nominated him 6 months ago, is another example of how extreme Senate Republicans have gone in their efforts to obstruct judicial confirmations. If they succeed in their partisan filibuster, it will be another first for them. Never before has the Senate filibustered and refused to vote on a judicial nominee with such strong bipartisan support, who was voted out of the Judiciary Committee with virtually unanimous support.

Their partisan efforts to shut down Senate confirmations of qualified judicial nominees who have bipartisan support do not help the American people. This is a shortsighted policy at a time when the judicial vacancy rate remains more than twice what it was at this point in the first term of President Bush. Judicial vacancies during the last few years have been at historically high levels. Nearly one out of every 11 Federal judgeships is currently vacant. Their shutting down confirmations for consensus and qualified circuit court nominees is not helping the overburdened Federal courts to which Americans turn for justice.

Over his 13-year career as a U.S. Magistrate Judge in the Western District of Oklahoma, Judge Robert Bacharach has handled nearly 3,000 civil and criminal matters, presided over 400 judicial settlement conferences, and issued more than 1,600 reports and recommendations. As an attorney in private practice, Judge Bacharach tried 10 cases to verdict, argued 2 cases before the Tenth Circuit Court of Appeals, and briefed scores of other cases to the tenth circuit and the Oklahoma Supreme Court. The ABA Standing Committee on the Federal Judiciary has rated Judge Bacharach unanimously well qualified, the highest possible rating from its nonpartisan peer review.

Judge Bacharach's judicial colleagues in the Western District of Oklahoma stand strongly behind his nomination. Vicki Miles-LaGrange, Chief Judge of the U.S. District Court for the Western District of Oklahoma, has said of Judge Bacharach:

He is an outstanding jurist and my colleagues and I enthusiastically and wholeheartedly recommend him for the Tenth Circuit position . . . We knew that we were lucky to have Bob as a Magistrate Judge, and he's been remarkable in this position for over 12 years. He is an absolutely great Magistrate Judge. His research and writing are excellent, his temperament is superb, his preparation is top-notch, and he is a wonderful colleague to all of the judges and in general to the entire court family. . . . All of the other judges and I—Republicans and Democrats alike—enthusiastically and wholeheartedly recommend Judge Bob Bacharach for the Tenth Circuit position. All of us believe very strongly that Judge Bacharach would be a superb choice for the position.

Throughout this very careful and deliberate process in which Judge Robert Bacharach has been thoroughly vetted, considered, and voted on by the Judiciary Committee, I have not heard a single negative word about him. There is no Senator that I know of who is opposed to his nomination on the merits. The only obstacle standing between Judge Bacharach being confirmed to serve the people of the tenth circuit is partisan obstruction.

Nor is Judge Bacharach the only victim of this abuse. In a letter dated June 20, 2012, the president of the American Bar Association urged Senator REID and Senator MCCONNELL to work together to schedule votes on the nominations of William Kayatta and Richard Taranto, as well as Judge Bacharach. These are three consensus, qualified circuit court nominees awaiting Senate confirmation so that they may serve the American people. I ask that a copy of that letter be printed in the RECORD, along with an article from the Oklahoman on this nomination.

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

AMERICAN BAR ASSOCIATION,
Chicago, IL, June 20, 2012.

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

DEAR MAJORITY LEADER REID AND REPUBLICAN LEADER MCCONNELL: Amid concerns that the judicial confirmation process is about to fall victim to presidential election year politics through the invocation of the ''Thurmond Rule,'' I am writing on behalf of the American Bar Association to reiterate our grave concern for the longstanding number of judicial vacancies on Article III courts and to urge you to schedule floor votes on three pending, noncontroversial circuit court nominees before July and on district court nominees who have strong bipartisan support on a weekly basis thereafter.

Three of the four circuit court nominees pending on the Senate floor are consensus nominees who have received overwhelming approval from the Senate Judiciary Committee. Both William Kayatta, Jr. of Maine, nominated to the First Circuit, and Robert Bacharach of Oklahoma, nominated to the Tenth Circuit, have the staunch support of their Republican senators. Richard Taranto, nominated to the Federal Circuit, enjoys strong bipartisan support, including the endorsement of noted conservative legal scholars. All three nominees also have stellar professional qualifications and each has been rated unanimously ''well-qualified'' by the ABA's Standing Committee on the Federal Judiciary.

As you know, the ''Thurmond Rule'' is neither a rule nor a clearly defined event. While the ABA takes no position on what invocation of the ''Thurmond Rule'' actually means or whether it represents wise policy, recent news stories have cast it as a precedent under which the Senate, after a specified date in a presidential election year, ceases to vote on nominees to the federal circuit courts of appeals. We note that there has been no consistently observed date at which this has occurred during the presidential election years from 1980 to 2008. With regard to the past three election years, the last circuit court nominees were confirmed in June during 2004 and 2008 and in July during 2000. In deference to these historical cut-off dates and because of our conviction that the Senate has a continuing constitutional duty to act with due diligence to reduce the dangerously high vacancy rate that is adversely affecting our federal judiciary, we exhort you to schedule votes on these three outstanding circuit court nominees this month.

We also urge you to continue to work together to move consensus district court nominees to the floor for a vote throughout the rest of the session, lest the vacancy crisis worsens in the waning months of the 112th Congress. With five new vacancies arising this month and an additional five announced for next month, this is not just a possibility; it is a certainty, absent your continued commitment to the federal judiciary and steady action on nominees.

Thank you for your past efforts and for your consideration of our views on this important issue.

Sincerely,

WM. T. (BILL) ROBINSON III,
President.

[From the Oklahoman, June 15, 2012]

SENATE REPUBLICANS TO BLOCK VOTE ON OKLAHOMA NOMINEE FOR FEDERAL APPEALS COURT

(By Chris Casteel)

WASHINGTON.—Senate Republicans won't allow a vote before November's presidential election to confirm U.S. Magistrate Judge Robert E. Bacharach to a federal appeals court, despite Bacharach's credentials and support from both Oklahoma senators, Sen. Tom Coburn said Thursday.

Coburn, R–Muskogee, said Senate Republican leader Mitch McConnell told him Republicans were following a tradition used by both parties to block votes on circuit court nominees a few months before a presidential election.

That means a vote on Bacharach, whose nomination to the 10th U.S. Circuit Court of Appeals cleared the Senate Judiciary Committee last week, ''is not going to happen,'' Coburn said.

Coburn said the nomination of John E. Dowdell to be a U.S. district judge in Tulsa still has a ''great chance'' of clearing the full Senate.

Bacharach is ''an awfully good candidate'' for the circuit court position, said Coburn, who praised his character and judicial temperament. Bacharach, who has been a magistrate judge in Oklahoma City since 1999, was given a rating of ''unanimously well qualified'' for the appeals court position by the American Bar Association.

Sen. Jim Inhofe, R–Tulsa, praised Bacharach during a committee hearing last month.

But the selection and confirmation process moved too slowly to fill the vacancy on the appeals court—which is a step below the U.S. Supreme Court—given the political timetable in Washington.

Though the position has been open since July 2010, the White House didn't make a nomination until January, after spending months vetting candidates that weren't going to be acceptable to Coburn and Inhofe.

Then, it took more than three months to schedule a committee hearing for Bacharach as the staff conducted a background investigation; Coburn withheld his approval for a committee hearing until the committee investigation was completed.

Ultimately, Bacharach may have just narrowly missed a full Senate vote. The Senate this week, over the objections of most Republicans, confirmed a nominee from Arizona for another circuit court. After that vote, McConnell told Republican senators no other votes on circuit judges would be held.

McConnell's office declined to comment on Thursday.

Sen. Patrick Leahy, D–Vermont, chairman of the Senate Judiciary Committee, said Thursday, ''This is really a challenge to the senators who have said that they will not support these filibusters and this kind of shutdown, and to those Republican senators who support the circuit court nominees from Maine and Oklahoma.''

But Coburn said there wasn't anything he could do about the situation.

The delaying tactic on circuit court judges, which will likely extend to district court judges later this year, has become common practice for the party that doesn't control the White House.

This year, it means Republicans will block votes on nominees for appeals courts, which can have great influence on a wide range of legal issues since the Supreme Court agrees to hear relatively few cases.

The aim of the tactic is to delay making lifetime appointments to federal courts in hopes their party will regain the White House and the power to fill judicial vacancies. Coburn said Bacharach could be cleared late this year if President Barack Obama wins re-election. If not, Coburn said, Bacharach would make a great nominee for a Republican president.

Mr. LEAHY. The ABA president wrote:

Amid concerns that the judicial confirmation process is about to fall victim to presidential election year politics through the invocation of the ''Thurmond Rule,'' I am writing on behalf of the American Bar Association to reiterate our grave concern for the longstanding number of judicial vacancies on Article III courts and to urge you to schedule floor votes on three pending, noncontroversial circuit court nominees before July and on district court nominees who have strong bipartisan support on a weekly basis thereafter.

This is the precise danger that was the reason for that letter. Including Judge Bacharach, William Kayatta of Maine, and Richard Taranto, there are currently 20 judicial nominees voted out of the Judiciary Committee and being blocked by Senate Republicans.

During the Judiciary Committee meeting approving the nomination of Judge Bacharach, Senator COBURN noted:

I believe that Judge Bacharach will uphold the highest standards and reflect the best in our American judicial tradition by coming to the bench as a well-regarded member of the community. At a time when our country seems as divided as ever, it is important that citizens respect members of the judiciary and are confident they will faithfully and impartially apply the law. . . I believe Judge Bacharach would be an excellent addition to the Tenth Circuit.

Senator INHOFE likewise has said: ''I believe that Judge Bacharach would continue the strong service Oklahomans have provided the Tenth Circuit.'' When asked last month about this effort to block a vote on Judge Bacharach's nomination, Senator COBURN told The Oklahoman: ''I think it's stupid.'' He is right. It is just obstruction.

There is no good reason that the Senate should not vote on consensus circuit court nominees thoroughly vetted, considered and voted on and approved with nearly unanimous bipartisan support by the Judiciary Committee. There is no reason the Senate cannot vote on the nomination of William Kayatta of Maine to the first circuit, a nominee strongly supported by both of Maine's Republican Senators and reported nearly unanimously by the committee 3 months ago and 2 months before considering Judge Bacharach's nomination. This is the same person who Chief Justice John Roberts recommended to Kenneth Starr for a position in the Justice Department. He is widely respected in Maine. Republicans cannot seriously oppose his nomination on the merits or for ideological reasons. It is just more obstruction.

There is also no reason the Senate cannot vote on Richard Taranto's nomination to the Federal circuit. He was reported almost unanimously by voice vote nearly 4 months ago, and is supported by conservatives such as Robert Bork and Paul Clement. Republicans cannot seriously oppose his nomination to the Federal circuit on the merits or for ideological reasons. It is just more obstruction.

Each of these circuit court nominees has been rated unanimously well qualified by the nonpartisan ABA Standing Committee on the Federal Judiciary, the highest possible rating. These are not controversial nominees. They are qualified and should be considered as consensus nominees and confirmed. Senate Republicans are blocking consent to vote on superbly qualified circuit court nominees with strong bipartisan support. This is a new and damaging application of the Thurmond rule.

It is hard to see how this new application of the Thurmond rule is really anything more than another name for the stalling tactics we have seen for months and years. I have yet to hear any good reason why we should not continue to vote on well-qualified, consensus nominees, just as we did up until September of the last 2 Presidential election years. I have yet to hear a good explanation why we cannot work to solve the problem of high vacancies for the American people. I will continue to work to confirm as many of President Obama's qualified judicial nominees as possible to fill the many judicial vacancies that burden our courts and the American people across the country.

Senate Republicans have become the party of no—no help for the American people, no to jobs, no to economic recovery, no help to extend tax cuts for the middle class, and no to judges to provide Americans with justice in their Federal courts. Although the public announcement that they would be blocking qualified and consensus circuit court nominees was not until June, the truth is that Senate Republicans have been obstructing President Obama's judicial nominees since the beginning of his Presidency, beginning with their filibuster of his first nominee.

Senate Republicans used to insist that filibustering of judicial nominations was unconstitutional. The Constitution has not changed but as soon as President Obama was elected they reversed course and filibustered President Obama's very first judicial nomination. Judge David Hamilton of Indiana was a widely respected 15-year veteran of the Federal bench nominated to the seventh circuit and was supported by Senator DICK LUGAR, the longest-serving Republican in the Senate. They delayed his confirmation for 5 months. Senate Republicans then proceeded to obstruct and delay just about every circuit court nominee of this President, filibustering nine of them. They delayed confirmation of Judge Albert Diaz of North Carolina to the fourth circuit for 11 months. They delayed confirmation of Judge Jane Stranch of Tennessee to the sixth circuit for 10 months. They delayed confirmation of Judge Ray Lohier of New York to the second circuit for 7 months. They delayed confirmation of Judge Scott Matheson of Utah to the tenth circuit and Judge James Wynn, Jr. of North Carolina to the fourth circuit for 6 months. They delayed confirmation of Judge Andre Davis of Maryland to the fourth circuit, Judge Henry Floyd of South Carolina to the fourth circuit, Judge Stephanie Thacker of West Virginia to the fourth circuit, and Judge Jacqueline Nguyen of California to the ninth circuit for 5 months. They delayed confirmation of Judge Adalberto Jordan of Florida to the eleventh circuit, Judge Beverly Martin of Georgia to the eleventh circuit, Judge Mary Murguia of Arizona to the ninth circuit, Judge Bernice Donald of Tennessee to the sixth circuit, Judge Barbara Keenan of Virginia to the fourth circuit, Judge Thomas Vanaskie of Pennsylvania to the third circuit, Judge Joseph Greenaway of New Jersey to the third circuit, Judge Denny Chin of New York to the second circuit, and Judge Chris Droney of Connecticut to the second circuit for 4 months. They delayed confirmation of Judge Paul Watford of California to the ninth circuit, Judge Andrew Hurwitz of Arizona to the ninth circuit, Judge Morgan Christen of Alaska to the ninth circuit, Judge Stephen Higginson of Louisiana to the fifth circuit, Judge Gerard Lynch of New York to the second circuit, Judge Susan Carney of Connecticut to the second circuit, and Judge Kathleen O'Malley of Ohio to the Federal circuit for 3 months.

As a recent report from the nonpartisan Congressional Research Service confirms, the median time circuit nominees have had to wait for a Senate vote has skyrocketed from 18 days for President Bush's nominees to 132 days for President Obama's circuit court nominees. This is the result of Republican foot dragging and obstruction. In most cases, Senate Republicans have been delaying and stalling for no good reason. How else do you explain the filibuster of the nomination of Judge Barbara Keenan of Virginia to the fourth circuit who was ultimately confirmed 99–0? And how else do you explain the needless obstruction of Judge Denny Chin of New York to the second circuit, who was filibustered for 4 months before he was confirmed 98–0?

The only change in their practices is that Senate Republicans have finally acknowledged that they are seeking to shut down the confirmation process for qualified and consensus circuit court nominees. Three of the five circuit court judges finally confirmed this year after months of unnecessary delays and a filibuster should have been confirmed last year. The other two circuit court nominees confirmed this year were both subjected to stalling and partisan filibusters, which were thankfully unsuccessful.

The American people need to understand that Senate Republicans are stalling and filibustering judicial nominees supported by their home State Republican Senators. Just consider the States I have already mentioned as having circuit nominees supported by their home State Republican Senators unnecessarily stalled—Indiana, North Carolina, Utah, South Carolina, Georgia. Just last month we needed to overcome a filibuster to confirm

Justice Andrew Hurwitz of the Arizona Supreme Court to the ninth circuit despite the strong support of Senators JON KYL and JOHN MCCAIN. Now it is nominees from Oklahoma and Maine who are being filibustered despite the support of their home State Republican Senators.

The year started with the majority leader having to file cloture to get an up-or-down vote on Judge Adalberto Jordan of Florida to the eleventh circuit even though he was strongly supported by his Republican home State Senator. And every single one of these nominees for whom the majority leader was forced to file cloture this year was rated unanimously well qualified by the nonpartisan ABA Standing Committee on the Federal Judiciary, the highest possible rating. Most were to fill a judicial emergency vacancy. So when I hear some Senate Republicans say they are now invoking the Thurmond rule and have decided they are not going to allow President Obama's judicial nominees to be considered, I wonder how the American people are supposed to be able to tell the difference from how they have been obstructing for the last 3½ years.

The minority's stalling of votes on judicial nominees with significant bipartisan support is all to the detriment of the American people. This has been a tactic that they have employed for the last 3½ years, despite repeated appeals urging them to work with us to help solve the judicial vacancy crisis. We have seen everyone from Chief Justice John Roberts, himself appointed by a Republican President, to the nonpartisan American Bar Association urging the Senate to vote on qualified judicial nominees who are available to administer justice for the American public. Sadly, Republicans insist on being the party of no.

What the American people and the overburdened Federal courts need are qualified judges to administer justice in our Federal courts, not the perpetuation of extended, numerous vacancies. Today vacancies on the Federal courts are more than 2½ times as many as they were on this date during the first term of President Bush. The Senate is more than 40 confirmations off the pace we set during President Bush's first term.

Because they cannot deny the strength of this comparison—using apples to apples by comparing first terms—Senate Republicans instead try to draw comfort by making comparisons to President Bush's second term after we had already worked hard to reduce vacancies by 75 percent. In fact, during President Bush's second term, the number of vacancies never exceeded 60 and was reduced to 34 near the end of his Presidency. In stark contrast, vacancies have long remained near or above 80, with little progress made in these last 3½ years. Today, there are still 76 vacancies. Their tactics have actually led to an increase in judicial vacancies during President Obama's first term—a development that is another sad first.

But the real point is that their selective use of numbers does nothing to help the American people. We should be doing better. I know that we can because we have done better. During President Bush's first term, notwithstanding the 9/11 attacks, the anthrax attack on the Senate, the ideologically driven selections of judicial nominees by President Bush, and his lack of outreach to home State Senators, we reduced the number of judicial vacancies down to 29 by this point during his first term and acted to confirm 205 circuit and district court nominees by the end of his first term.

Another excuse from the minority comes across more as partisan score settling than anything else. They claim that having confirmed two Supreme Court Justices, the Senate cannot be expected to reach the 205 number of confirmations in President Bush's first term.

But those Supreme Court confirmation proceedings from years ago do not excuse the Senate from taking the actions it could now on the 20 judicial nominees voted out of the Judiciary Committee and ready for final Senate action. That second Supreme Court confirmation was in August 2010. That is almost 2 years ago and it was opposed by most Senate Republicans.

Senate Republicans held down circuit and district court confirmations in President Obama's first 2 years in office to historically low numbers—12 by the end of 2009 and another 48 in 2010 for a total of only 60. They refused to act on 10 nominees ready at the end of 2009 and on 19 as 2010 drew to a close. Last year they employed the same tactic in stalling action on another 19 judicial nominees at the end of 2011. Now it is 20 judicial nominees in this summer of 2012 that they are stalling. Had Republicans not stalled 19 nominations at the end of last year and dragged those confirmations out into May of this year, we the American people and the Federal courts would be much better off. As it is, however, the fact remains that there are 20 qualified judicial nominations that the Senate could be voting on without further delay.

They refuse to acknowledge that in addition to confirming two Supreme Court Justices in President Clinton's first term, the Senate was able to confirm 200 circuit and district court judges. And in 1992, at the end of President George H.W. Bush's term, the Senate with a Democratic majority was able to confirm 192 circuit and district court judges despite confirming two Supreme Court Justices. Republicans have kept the Senate well back from those numbers by only allowing the Senate to proceed to confirm 154 of President Obama's circuit and district court nominees. That is a far cry from what we have been able to achieve in addition to our consideration of Supreme Court nominations when the Senate was being allowed to function more fairly and to consider judicial nominees reported with bipartisan support.

Nor are the nominees about whom we are concerned recently nominated. These are not nominees dumped on the Senate in scores at the end of a Presidential term. These are, instead, nominations that date back to October of last year. Most were nominated before March. In fact the circuit court nominees who Republicans are refusing to consider date back to October and November of last year and January of this year. William Kayatta was voted on by the committee and placed before the Senate by mid-April and could have been confirmed then. Richard Taranto and Judge Patty Shwartz have been stalled before the Senate even longer, since March. The truth is that Senate Republicans have shut down confirmations of circuit court judges not just in July but, in effect, for the entire year. The Senate has yet to vote on a single circuit court nominee nominated by President Obama this year. Since 1980, the only Presidential election year in which there were no circuit nominees confirmed who was nominated that year was in 1996, when Senate Republicans shut down the process against President Clinton's circuit nominees. The fact that Republican stalling tactics have meant that circuit court nominees that should have been confirmed in the spring—like Bill Kayatta, Richard Taranto and Patty Shwartz—are still awaiting a vote after July 4th is no excuse for not moving forward this month to confirm these circuit nominees.

The American people who are waiting for justice do not care about excuses. They do not care about some false sense of settling political scores. They want justice, just as they want action on measures the President has suggested to help the economy and create jobs rather than political calculations about what will help Republican candidates in the elections in November.

When Republican Senators try to take credit for the Senate having reached what they regard as their ''quota'' for confirmations this year, they should acknowledge their strenuous opposition and attempts to filibuster many of the nominations for which they now take credit. As recently as 2008, Senate Republicans denied there was a Thurmond rule. They used to say that any judicial nominee reported by the Senate was entitled to an up-or-down vote and that they would never filibuster judicial nominees. Well, the majority leader has had to file 30 cloture petitions to end their filibusters of judicial nominees. Now they are flip-flopping on their own call for up-or-down votes.

What they are doing now is a first. As I have noted, in the past 5 Presidential election years, Senate Democrats have never denied an up-or-down vote to any circuit court nominee of a Republican President who received bipartisan support in the Judiciary Committee. They

are denying votes not only to Robert Bacharach, a nominee from Oklahoma supported by his conservative home State Republican Senators but also to William Kayatta, a universally respected nominee from Maine supported by his home State Republican Senators, and Richard Taranto, whose nomination to the Federal circuit received virtually unanimous support. Even Judge Patty Shwartz, whose nomination to the third circuit received a split rollcall vote, has the bipartisan support of New Jersey Governor Chris Christie.

Personal attacks on me, taking quotes out of context, trying to repackage their own actions as if following the Thurmond rule or what they seek to dub the Leahy Rule do nothing to help the American people who are seeking justice in our Federal courts. I am willing to defend my record but that is beside the point. The harm to the American people is what matters. Republicans are insisting on being the party of no even when it comes to judicial nominees who home State Republican Senators support.

As chairman and when I served as the ranking member of the Judiciary Committee, I have worked with Senate Republicans to consider judicial nominees well into Presidential election years. I have taken steps to make the confirmation process more transparent and fair. I have ensured that the President consults with home State Senators before submitting a nominee. I have opened up what had been a secretive, blue-slip process to prevent abuses. All the while I have protected the rights of the minority, of Republican Senators. If Republicans want to talk about the Leahy rules, those are the practices I have followed. And I have been consistent. I hold hearings at the same pace and under the same procedures whether the President nominating is a Democrat or a Republican. Others cannot say that.

Senate Republicans are fond of taking quotes of things I have said out of context. But look at my record as chairman. I have not filibustered nominees with bipartisan support in July of Presidential election years. As chairman of this committee, I have steadfastly protected the rights of the minority. I have done so despite criticism from Democrats. I have only proceeded with judicial nominations supported by both home State Senators. I will put my record of consistent fairness up against that of any chairman and remind Senate Republicans that it is they who blatantly disregarded even-handed practices when they were ramming through ideological nominations of President George W. Bush. They would proceed with nominations despite the objection of both home State Senators.

So those are the Leahy rules—respect for and protection of minority rights, increased transparency, consistency, and allowing for confirmations well into Presidential election years for nominees with bipartisan support.

And what were the results? In the last two Presidential election years, we were able to bring the number of judicial vacancies down to the lowest levels in the past 20 years. In 2004, at the end of President Bush's first term, vacancies were reduced to 28, not the 76 we have today. In 2008, in the last year of President Bush's second term, we again worked to fill vacancies and got them down to 34, less than half of what they are today. In 2004, 25 nominees were confirmed from June 1 to the Presidential election. In 2008, 22 nominees were confirmed between June 1 and the Presidential election. So far, since June 1 of this year, only eight judges have been confirmed and five required the majority leader to file cloture to end Republican filibusters.

In 2004, the Senate confirmed five circuit court nominees of a Republican President that had been reported by the committee that year. This year we have confirmed only two circuit court nominees that have been reported by the committee this year, and we had to overcome Republican filibusters in both cases. By this date in 2004 the Senate had already confirmed 35 of President Bush's circuit court nominees. So far, the Senate has only been allowed to consider and confirm 30 of President Obama's circuit court nominees—5 fewer, 17 percent fewer—while higher numbers of vacancies remain, and yet the Senate Republican leadership demands an artificial shutdown on confirmation of qualified, consensus nominees for no good reason.

In fact, during the last 20 years, only four circuit nominees reported with bipartisan support have been denied an up-or-down vote during a Presidential election year by the Senate; all four were nominated by President Clinton and blocked by Senate Republicans. While Senate Democrats have been willing to work with Republican Presidents to confirm circuit court nominees with bipartisan support, Senate Republicans have repeatedly obstructed the nominees of Democratic Presidents. In the previous 5 Presidential election years, a total of 13 circuit court nominees have been confirmed after May 31. Not surprisingly, 12 of the 13 were Republican nominees. Clearly, this is a one-way street in favor of Republican Presidents' nominees.

Senate Republicans, on the other hand, have repeatedly asserted that the Thurmond rule does not exist. For example, on July 14, 2008, the Senate Republican caucus held a forum and said that the Thurmond rule does not exist. At that meeting, the senior Senator from Kentucky, the Republican leader stated: ''I think it's clear that there is no Thurmond rule. And I think the facts demonstrate that.'' Similarly, the Senator from Iowa, my friend who is now serving as ranking member of the Judiciary Committee, stated that the Thurmond rule was in his view ''plain bunk.'' He said: ''The reality is that the Senate has never stopped confirming judicial nominees during the last few months of a President's term.'' We did not in 2008 when we proceeded to confirm 22 nominees over the second half of that year.

So at the end of President Bush's second term, and at the beginning of his first term as well, Senate Democrats worked to confirm consensus nominees and reduce the judicial vacancy rate. Despite the pace we set during President Bush's first term for reducing vacancies, vacancies have remained near or above 80 for most of President Obama's first term and little comparative progress has been made during the three and a half years of President Obama's first term. As contrasted to 29 vacancies in July 2004, there are still 76 vacancies in July 2012. If we could move forward to Senate votes on the 20 judicial nominees ready for final action, the Senate could reduce vacancies to less than 60 and make some progress. We were 9 months later in confirming the 150th circuit or district judge to be appointed by President Obama. Another way to look at our relative lack of progress and the burden the Republican obstruction is placing on the American people seeking justice is to note that by mid-November 2002 we had already reduced judicial vacancies to below where we are now. In fact, when on November 14, 2002, the Senate proceeded to confirm 18 judicial nominees, vacancies went down to 60 throughout the country. We effectively worked twice as efficiently and twice as fast. By that measure, the Senate is almost 20 months behind schedule. This is hardly then the time to be shutting down the process.

In a letter to Senators COBURN and INHOFE dated July 19, 2012, the American Bar Association's State Delegate for Oklahoma urged the Republican Senators to rise above politics and to end this filibuster of Judge Bacharach. I ask unanimous consent that a copy of this letter be printed in the RECORD.

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

AMERICAN BAR ASSOCIATION,
Oklahoma City, OK, July 19, 2012.

Senator JAMES M. INHOFE,
Russell Senate Office Building, Washington, DC.

Senator TOM COBURN,
Russell Senate Office Building, Washington, DC.

DEAR SENATORS INHOFE AND COBURN: The undersigned, Oklahoma's current delegates to the American Bar Association (ABA) (less two judge members who abstain from this letter), are writing to ask you respectfully to press the Republican Senate leadership for a floor vote, before the traditional August recess, on the nomination of Judge Robert Bacharach to the Tenth Circuit Court of Appeals vacancy.

As you probably know, the ABA wrote to the Senate leaders of both parties on June 20, 2012, after Senator McConnell announced his party's intention to invoke the so-called ''Thurmond Rule'' and block floor consideration of any more nominees to any federal circuit court vacancies, including those, like Judge Bacharach, that: (1) have passed through the Judiciary Committee; (2)

present no controversy on their qualifications; and (3) have the support of their home state senators.

We appreciate your role in the selection of Judge Bacharach and your public support for his nomination. As you know, he has been rated ''unanimously well qualified'' by the ABA panel that reviewed his qualifications.

We understand that both political parties have engaged in a variety of stalling tactics, including the threat of a filibuster, regarding judicial nominations in the past. However, this ignores the fact that this Oklahoma slot on the Tenth Circuit has now been vacant for over two years.

Therefore, we are asking you (1) to use your considerable influence within the Senate and urge the leadership of both parties to schedule a floor vote on Judge Bacharach's nomination before the August recess, and (2) to publicly announce your willingness to vote to end any filibuster preventing a vote on the merits of the nomination, if necessary.

Respectfully,

JIMMY GOODMAN,
ABA State Delegate for Oklahoma.

For himself and also for: Cathy M. Christensen, OBA (OK Bar Assoc.) President; William G. Paul, ABA Past President; Dwight L. Smith, ABA Division Delegate; James T. Stuart, OBA President-Elect; M. Joe Crosthwait, Jr., Okla. County Bar Delegate; Mark A. Robertson, ABA Section Delegate; Peggy Stockwell, OBA Vice President; Robert S. Farris, Tulsa County Bar Delegate; Jennifer Kirkpatrick, Young Lawyer Delegate.

Mr. LEAHY. Mr. President, it is time for reasonable and independent thinking Senators to end this needless and damaging filibuster on Judge Bacharach's nomination and confirm him. With judicial vacancies remaining at such high levels for so long, we need to continue confirming judicial nominees. At a time when judicial vacancies remained historically high for 3 years, with 40 more vacancies and 40 fewer confirmations than at this point in President Bush's first term, the Senate Republican leadership should reconsider its obstruction and work with us to fill these longstanding judicial vacancies in order to help the American people. We have well-qualified, consensus nominees with bipartisan support who can fill these vacancies. It is only partisan politics and continued tactics of obstruction that stand in the way.

Mr. FRANKEN. Mr. President, I ask unanimous consent that any time in a quorum call be equally divided.

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

Mr. FRANKEN. Mr. President, 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. GRASSLEY. 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. GRASSLEY. Mr. President, for the last few weeks, it has been routine practice here in the Senate that we vote on consensus district court nominees most Mondays. We have done so quite a number of times in this Congress. We could have done so again tonight. Instead, the majority leader has decided to pursue another course. Rather than confirm what would have been the 155th judge tonight, the majority will instead engage in a political activity. Make no mistake, it is purely and simply a political posturing situation. It is really unfortunate.

It is well known that the practice and tradition of the Senate is to stop confirming circuit nominees in the closing months of a Presidential election year. That is what we have done during the last number of Presidential election years. That started in 1980, I believe. So that would be 32 years. In fact, today is July 30. You would have to go back that number of years to find a Presidential election year when we approved a circuit court judge this late.

Of course, the rationale has been that this close to an election, whoever wins that election should be the one to pick these lifetime nominees who will run our judiciary system. It is true that there were some votes in relation to circuit nominations in July during the last two election years. The only problem, of course, is that those were cloture votes on outstanding nominees the Democrats were filibustering.

For example, in July 2004—remember, that was a Presidential election year—cloture votes were held on four outstanding circuit nominees the Democrats were filibustering. Those included Miguel Estrada, nominated for the D.C. Circuit; Richard Griffin, nominated to the sixth circuit court; David McKeagh, nominated to the sixth circuit; and Henry Saad, also nominated to the sixth circuit.

I would note that at the time the sixth circuit alone had a 25-percent vacancy rate. And every one of those vacancies was designated as judicial emergencies.

That, of course, didn't matter to the other side. Despite the fact that the sixth circuit was in dire straits, the other side filibustered every one of those nominees.

I don't recall too much concern from my friends on the other side of the aisle about the need to confirm those judges.

And now, when our side seeks to enforce the rule the other side helped create and perfect, all we hear are complaints.

Mr. President, if ever there was an example of ''crocodile tears,'' this is it.

In 2008, the other side was at it again. Once again, they closed-up shop on Circuit nominations in June. This time, it was the Fourth Circuit that was in dire straits.

Despite the fact that the Fourth Circuit was 25 percent vacant, the Democrats refused to even process four outstanding consensus nominees.

Those nominees included Judge Robert Conrad, even though he had already been confirmed unanimously as a U.S. Attorney and District Court Judge. Democrats refused to process Judge Glen Conrad even though he had strong bipartisan home state support. Steve Matthews also had strong home-state support yet the Democrats in Committee refused to give him a vote. To show you the incredible lengths the Democrats were willing to go, they even tried to justify blocking the nomination of U.S. Attorney Rod Rosenstein to the fourth circuit by claiming he was doing ''too good of a job'' as U.S. Attorney to be promoted.

By refusing to give these nominees a vote in Committee, the Democrats engaged in what amounted to a ''pocket filibuster'' of all four of these candidates to the fourth circuit.

And again, this was at a time when the fourth circuit's vacancy rate was over 25 percent, similar to the Sixth Circuit vacancy rate in 2004. But that didn't matter to the other side. In 2008, just like in 2004, they simply refused to process any more circuit nominees after June.

At the end of the day, based on any fair and objective metric, the suggestion that we today are operating any differently than Democrats did in 2004 and 2008 is simply without merit. Democrats stalled and blocked numerous highly qualified circuit nominees during those Presidential election years including even nominees with bipartisan support.

The Democratic leadership has invoked repeatedly what has been called the ''Thurmond Rule'' to justify stalling nominees—even those with bipartisan support. And now they don't want us to play by the same set of rules. The Democratic leadership doesn't want us to enforce the rule that they helped establish.

Let me quote from a CRS report on this subject:

> The Senator who most frequently has asserted the existence of a Thurmond rule has been the current chairman of the Judiciary Committee.

The CRS report noted that on March 7, 2008, the Chairman recalled:

> When President Reagan was running for President and Senator Thurmond, then in the Republican minority as ranking member of the Judiciary Committee, instituted a policy to stall President Carter's nominations. That policy, known as the ''Thurmond Rule,'' was put in when the Republicans were in the minority. It is a rule that we still follow, and it will take effect very soon here.

Again, this was in March of that Presidential election year, not June or July.

CRS went on to note the strong support the majority leader has expressed for the so-called Thurmond rule. According to CRS:

> Senator Harry Reid, the Senate majority leader, has expressed agreement with Senator Leahy about the existence of a Thurmond rule. In April 10, 2008, floor remarks, Senator Reid said, ''In a Presidential election year, it is always very tough for judges. That is the way it has been for a long time, and that is why we have the Thurmond rule and other such rules.''

Five days later, the Majority Leader said:

You know, there is a Thurmond doctrine that says: After June, we will have to take a real close look at judges in a Presidential election year.

These quotes indicate not only the expectation, but in fact a support for slowing down and cutting off the confirmation of judges in a Presidential election year.

Senate Republicans are invoking this practice in a more narrow fashion, and after more confirmations than Democrats did in the past.

Setting aside the so-called Leahy-Thurmond rule, by any objective measure, this President has been treated fairly and consistent with past Senate practices.

For example, with regard to the total number of confirmations, this President is well ahead of his predecessor. We have confirmed 154 of this President's district and circuit nominations. We have also confirmed 2 Supreme Court nominations during President Obama's first term. When Supreme Court nominations are pending in the Committee, all other nominations work is put on hold.

The last time the Senate confirmed two Supreme Court nominees was during President Bush's second term. And during that term the Senate confirmed a total of only 119 district and circuit court nominees.

Let me put it another way, under similar circumstances, we have confirmed 35 more district and circuit nominees for President Obama than we did for President Bush.

During the last Presidential election year, 2008, the Senate confirmed a total of 28 judges—24 district and 4 circuit. This Presidential election year we have already exceeded those numbers, having confirmed a total of 32 judges. So those who say that this President is being treated differently either fail to recognize history, or want to ignore the facts, or both.

While this President has not been treated differently than previous Presidents, he certainly has behaved differently with regard to nominations. He has been slow to send nominees to the Senate, and he abused his recess appointment authority. If President Obama hasn't gotten as many confirmations as he could have, it is because he has been slow to nominate and he has abused his recess appointment power.

Let me take just a moment to discuss how slow the President has been with his nominations.

When President Obama took office, there were 59 judicial vacancies. One year earlier, at the beginning of 2008, there were only 43 vacancies. So, during the last year of President Bush's second term, when the Democrats controlled the Senate, and during a time when they refused to process four nominees for the fourth circuit, they allowed the vacancy rate to increase by more than 37 percent.

By mid-March 2009, when the first Obama judicial nomination was sent up to the Senate, there were 70 judicial vacancies. Over the next 3 months, only five more circuit nominations were sent to the Senate. By the end of June, when the Senate received its first district nomination, there were 80 vacancies.

The failure or delay in submitting nominations for vacancies has been the practice of this administration and it still continues to this day.

By the end of 2009, there were 100 vacancies, with only 20 nominees. In December 2010, more than half of the 108 vacancies had no nominee. At the beginning of this year, only 36 nominees were pending for the 82 vacancies. And it continues to this day, more than half of the 76 vacancies have no nominee.

I just want to remind my colleagues that all of this begins with the White House. So if someone wants to complain about judicial vacancies, they should mail those complaints to 1600 Pennsylvania Avenue.

Now, I also mentioned that the President could have had a few more district court nominees at the end of last Congress.

Our side offered to confirm quite a number of district court nominees who were on the Executive Calendar, If the President would provide his assurances that he wouldn't bypass the Senate with recess appointments. The President refused to provide those assurances, and we found out why a couple weeks later when the President unconstitutionally bypassed the Senate.

I want everyone to understand that. At the end of last Congress we offered to confirm quite a few district court nominees. But the President wouldn't take ''Yes'' for an answer. Rather than choosing a path that led to more progress and a greater number of confirmations, the President chose the path to more confrontation and fewer confirmations.

The same thing happened last week. Once again, our side offered to confirm additional district court nominees. But, once again, the other side refused to take ''Yes'' for an answer. Rather than choosing the path that led to cooperation and additional confirmations, the other side chose more confrontation and fewer confirmations. They would rather waste precious time on a vote to nowhere, than spend the little time we have left on getting more nominations done. So here we are engaged in this political theater.

I urge my colleagues to vote ''No'' on cloture.

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

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

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

The PRESIDING OFFICER (Mr. TESTER). Without objection, it is so ordered.

Mr. MCCONNELL. Mr. President, it is almost August. We are just a few weeks away from the political parties' nominating conventions. At this point in past Presidential election years, the Senate is diligently working on things such as appropriations bills or the Defense authorization bill but not this year in the Senate.

Our Democratic colleagues refuse to do the basic work of government. Even though Chairman INOUYE has said he would like to pass some of the nine appropriations bills his committee has worked hard to complete, we haven't taken up a single one. Our Democratic colleagues will not bring the Defense authorization bill to the floor either, even though both the chairman and the ranking member of the Armed Services Committee are ready to work on this important legislation as well. And they refuse to work with us to help the economy or to prevent a looming tax hike on nearly 1 million small businesses at the end of the year.

Instead, they prefer to waste valuable time on a vote they have argued for many years shouldn't take place this close to a Presidential election. Now that there is a Democrat in the White House, they refuse to follow past practice on postponing the consideration of circuit court nominations this late in a Presidential election year so the American people can decide whom they want to make these important appointments. This practice is known as the Leahy-Thurmond rule. It is a custom they vigorously defended when there was a Republican in the White House.

So let's take a look at recent history. In 2004, the unemployment rate was only 5.4 percent. On our circuit courts, however, back in 2004, there were nine declared judicial emergencies. That didn't matter to our Democratic colleagues. The Senate stopped—stopped—circuit court nominations in June of that year, even though we had nine judicial emergencies. In 2008, the unemployment rate wasn't much higher, at 6.1 percent. In our circuit courts, there were almost as many judicial emergencies. But in the Fourth Circuit things were much worse: Fully one-fourth of the seats were empty, even though there were qualified nominees to fill them. Our Democratic colleagues didn't care then either. In the name of Senate custom and practice—by which I mean the Leahy-Thurmond rule—they pocket-filibustered several outstanding circuit court nominees in committee.

It didn't matter to our Democratic friends that these nominees enjoyed strong home State support, including bipartisan home State support, or that they had outstanding credentials or that they would fill declared emergencies on our circuit courts. The Senate couldn't process them—they told us again and again and again—because it was June and that was—to quote the chairman of the Judiciary Committee—''way past the time'' of the Leahy-Thurmond rule.

Today, it is August, not June, that is upon us. The country's unemployment

rate is, unfortunately, much higher than it was in either 2004 or 2008. It is now at 8.2 percent. But the situation on our circuit courts is much better than it was in either 2004 or 2008. There are now fewer judicial emergencies. In terms of what the Senate can do about it, as opposed to the President's failure to nominate people, we have confirmed—we have confirmed—every nominee whom the President has submitted to fill a judicial emergency on our circuit courts, save one—only one. That is right. The Senate has confirmed every nominee the President has sent to fill an emergency on our circuit courts, save one, and that one nominee isn't on the Senate floor.

In fact, the Senate has already confirmed as many or more circuit court nominees this year than it did in 2004 or 2008. It has confirmed a much higher percentage of circuit court nominations and it has confirmed those nominations faster than during the Bush administration.

On that last point, although we will not hear our Democratic friends acknowledge it, the average time from nomination to confirmation—the average time from nomination to confirmation—of a circuit court nominee for President Obama is over 1 month faster than it was for President Bush in his first term. Again, the time from nomination to confirmation for President Obama is over 1 month faster for a circuit court nominee than in President Bush's first term, and it is over 100 days faster than it was for President Bush's circuit court nominees overall.

So the situation with our economy is worse now than it was in 2004 or 2008, while the situation on our circuit courts is better. The economy is worse, but the situation on circuit courts is better. So what do you think our Democratic colleagues are going to focus on? Are they going to do the basic work of government—fund the government, for example? It doesn't look like it. Are they going to reauthorize important programs for our Nation's defense? I am told it has been 50-some-odd-years since the Defense authorization bill hasn't passed—no sign of it this year. Are they going to work with us to fix the economy or prevent a looming tax hike? I don't see any evidence of it yet.

What they want to do, instead, is violate the custom in Presidential election years that the Congressional Research Service says they have been the biggest proponents of. This is not me saying this, this is the Congressional Research Service. They want to violate the custom in Presidential election years that the CRS says they have been the biggest proponents of.

The CRS does not say the biggest proponent of the Leahy-Thurmond rule is me or Ranking Member GRASSLEY or even Senator Thurmond. Rather, the CRS says the most frequent proponent of the rule ''is the current chairman of the Senate Judiciary Committee.''

No doubt we will hear some post hoc, gerrymandered rationale from our Democratic friends as to why the rule the CRS says they have been the biggest proponents of somehow doesn't apply to them. They will ignore the pocket filibusters of people who would have filled judicial emergencies during a Republican administration. But, of course, that is par for the course.

Whether it is pro forma sessions to prevent recess appointments, or judicial filibusters, or the Leahy-Thurmond rule, our friends don't want the practices they have pioneered or been the biggest proponents of to apply to them. They don't want the practices they have been the pioneers of and the biggest proponents of to apply to them. Now it is pretty convenient for them, but that is not the way the Senate is supposed to work.

In sum, on the subject of the Leahy-Thurmond rule, we have been more responsible in deciding to invoke it in this year than our Democratic colleagues were in either 2004 or 2008. I would urge my friends to oppose this double standard and to oppose cloture.

Let me repeat. This is not about the individual who has been nominated. It wasn't, in many respects, about the individuals to be nominated in 2004 or 2008. What this is is a bipartisan timeout—bipartisan in the sense that it has been used by both sides—a timeout within, this year, 6 months of an election; in 2008, it was within 8 months of the end of a term—but within 6 months of an election to these important lifetime jobs to see who the next President may be.

Mr. INHOFE. Mr. President, will the Senator yield?

Mr. MCCONNELL. I yield to my friend from Oklahoma.

Mr. INHOFE. Let me first say it is awkward that one of the best nominees, Robert Bacharach, is the one subject to this. I regret that is the case. The problem is this would be the latest confirmation of a circuit court nominee during an election year in 20 years.

I was thinking today that I cannot vote against this guy, but I sure can vote present. If we have a 20-year precedent that was put in there by the Democrats and the Republicans alike, I wouldn't want to be the one to break that precedent. We are within 4 months of an election right now. It is very important that we do what we have done over the last 20 years and allow the new administration to come in.

The nomination of Robert Bacharach has been up there for 2 years before any action. You have to be a little suspicious as to why is he coming up right now. So I may end up voting present.

Mr. MCCONNELL. I thank my friend from Oklahoma. He confirms that this is not about the nominee, who apparently is well qualified. This is about an approach that has developed over several decades called the Leahy-Thurmond rule, under which it has been the practice to kind of call a timeout within rather close proximity to an election. In 2008, the timeout was called in June. We are going to enter August at the end of this week.

I would say also to my friend from Oklahoma, we have confirmed for the President in this election year five circuit court nominees. President Bush in 2008 got four; President Bush in 2004 got five. We have not been unfair to the administration. And it is certainly no reflection on what is apparently an outstanding nominee from your State.

Mr. President, I yield the floor.

The PRESIDING OFFICER. The Senator from Illinois.

Mr. DURBIN. Mr. President, I hope the American people are witnessing this moment in the Senate. We are about to make history. We are going to make history here in a few minutes when we have a rollcall vote on U.S. Magistrate Judge Robert Bacharach to the Tenth Circuit Court of Appeals. This fine man who has been nominated to this high position in the Federal judiciary has the support of both Senators of his home State. They are both Republicans.

Listen to what Senator TOM COBURN said of Mr. Bacharach: A stellar candidate. Listen to what Senator INHOFE said about this same nominee from his State: A great guy.

I listened to these comments. Then I reflect on the fact this man was reported out of the Senate Judiciary Committee on a voice vote. There was so little controversy because of his outstanding record, he was reported out on a voice vote.

The Democratic majority leader has offered to bring to the floor of the Senate a nominee approved by both Republican Senators from Oklahoma, and now you hear Senator MCCONNELL come to the floor and explain why the Republicans will have to filibuster and stop this man from being appointed to the court. Is it something about him? No. It is all about politics and it is all about the Presidential campaign.

If the Republicans sustain this filibuster and stop this good man from his service on the circuit court, it will be the first time in the history of the Senate that an appeals court nominee with bipartisan committee support has ever been filibustered on the floor of the Senate. But how can we be surprised? This will be the 86th Republican filibuster this Congress.

It is said that if the only tool you own is a hammer, every problem looks like a nail. If you happen to be a Republican leader in the Senate, every day looks like another chance for a filibuster. Eighty-six filibusters. Now they are filibustering judicial nominees approved nearly unanimously by the committee and approved by both Republican Senators. The President is prepared to assign this man into this position—a critically important position in the judiciary—and who is stopping him? The Republicans in the Senate, the 86th Republican Senate filibuster in this Congress. No surprise that it comes from Senator MCCONNELL, who very openly and candidly, and I assume honestly, said, My biggest job in the Senate is to make sure

Barack Obama is a one-term President. That is how he welcomed President Obama to the White House.

So they have piled filibuster on top of filibuster to stop the rare possibility that this President would give this good man, this exceptional man, a chance to serve his country. Listen to the background of this man who is about to become a victim of the 86th Republican filibuster:

For 13 years he has served as a federal magistrate. He has handled an impressive caseload, including almost 3,000 civil and criminal matters, and 400 judicial settlement conferences. He is the type of consensus nominee we look for in every single State. He has been given the highest possible rating by the American Bar Association. No questions asked, this is a good man and a good candidate for this job. In the American Bar Association's nonpartisan peer review, every single reviewer said this magistrate is well qualified to serve as a circuit court judge in the Tenth Circuit Court of Appeals. And where are the politics there? The politics are that the Democratic majority leader has offered to the two Republican Senators from Oklahoma a chance for this good man to serve, and now they are going to stop him with a Republican filibuster.

If you are looking for evidence of a dysfunctional Senate, hold on tight. In just a few moments we will start a rollcall, and you will watch as Republican after Republican comes and votes to kill this man's nomination for the Tenth Circuit Court of Appeals. President Obama will be the first President in 20 years to complete his first term with more judicial vacancies than when he took office. They have dragged their feet every step of the way with filibusters and delays to stop this President from appointing the judges he was elected to appoint. And good people—good people such as U.S. Magistrate Judge Robert Bacharach—who submit their names in this process, who go through extensive background investigations, who put their lives on hold wondering if they are going to make it, end up getting caught in a political game that is being played here on the floor.

I hope there is a handful—five, six, or seven—Republican Senators who will give this man a fair break and will give him a chance to serve his country as a circuit judge for the Tenth Circuit Court of Appeals. Please, let us not make history today by stopping a highly qualified bipartisan nominee, well qualified by the American Bar Association, from serving this circuit. The Republican Senators from Oklahoma are right—he is a stellar candidate and, by every measure, a great guy. Please don't make him a victim of last-minute political campaigning in this last week before the recess we take for our Democratic national convention and the Republican national convention. He shouldn't be a victim of this Presidential campaign. He deserves a chance to serve.

Mr. President, I yield the floor.

The PRESIDING OFFICER. The Senator from Alabama.

Mr. SESSIONS. Mr. President, I don't like to get involved in the back and forth on this issue. It bothers me. Chairman LEAHY goes into all these numbers, and they are distorted for the most part in connection with the reality. I have said that I simply will not, however, stand by and see the record misconstrued and the picture painted as something other than it is.

President Bush's judicial nominees were filibustered extraordinarily, unlike anything we had ever seen before. And this is the way it happened. I was here, I remember it very distinctly. President Bush was elected President. In 2001, shortly after he was elected, the New York Times reported that a group of well-known liberal law professors, including Laurence Tribe, Cass Sunstein, and Marsha Greenberger, met with Democratic Senators in a retreat. They proposed to the Democratic conference, who were then in the minority in the Senate—they didn't have the majority. President Bush was going to be nominating judges, and they decided to change the ground rules of judicial confirmation. That is a fact. After that, they aggressively executed a plan of unprecedented obstruction of judicial nominees.

In a totally unprecedented use of the filibuster, the Senate confirmed only 6 of 25 of President Bush's circuit court nominees. Two of those six were prior Clinton nominees President Bush, in an act of good faith, renominated. Of course they were immediately confirmed. Yet the majority of President Bush's first nominees to the circuit court waited years for confirmation. Many were never confirmed.

Perhaps the most disturbing story was that of Miguel Estrada, which has come up recently in the confirmation of Supreme Court Justices in which some of my Democratic colleagues basically acknowledge that he was unfairly treated. He is an outstanding appellate lawyer, supremely qualified to serve on the District of Columbia Circuit Court. He waited 16 months for a hearing. They would not give him a hearing.

This was all after 2000, in their determination to change the ground rules. Before that, filibusters had not been utilized against nominees, not to any degree. Almost never, actually. We had a fight over it. I spoke on maybe half a dozen or a dozen times about Mr. Estrada. There were seven cloture votes—seven attempts—by the Republicans to get a vote on Mr. Estrada so he could be confirmed. He was a superb nominee, and he was treated very poorly. It was not the right thing, and people have acknowledged it since.

Mr. President, is there a time agreement on the vote to commence?

The PRESIDING OFFICER. The time for the minority leader just expired.

Mr. SESSIONS. Mr. President, I ask unanimous consent to have one additional minute.

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

Let me just say this: In the last 20 years, going back even before this dispute began in 2000, when Democrats changed the ground rules of confirmations and started filibustering systematically qualified nominees, not one circuit judge has been confirmed after this day. That has been the tradition of the Senate. It has been referred to as the Thurmond rule. Maybe it would be even more appropriate to say the Leahy rule.

Others have talked about the quotes that have been made from Senator REID and Senator LEAHY on the floor. This is the tradition of the Senate that when someone is up for reelection, after this day, to get their nominees confirmed, they have to win reelection. If President Obama is successful in being reelected, I am sure he will have a high likelihood of getting this nominee and others confirmed.

I thank the Chair, yield the floor, and note the absence of a quorum.

The PRESIDING OFFICER (Mr. MANCHIN). The clerk will call the roll.

The assistant legislative clerk proceeded to call the roll.

The PRESIDING OFFICER. The Senator from Alabama.

Mr. SESSIONS. Mr. President, I ask unanimous consent that the quorum call be rescinded.

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

Mr. SESSIONS. Mr. President, I yield back all time prior to the vote.

CLOTURE MOTION

The PRESIDING OFFICER. Under the previous order, pursuant to rule XXII, the Chair lays before the Senate the pending cloture motion, which the clerk will report.

The assistant legislative 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.

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 nomination of Robert E. Bacharach, of Oklahoma, to be United States Circuit Judge for the Tenth Circuit, 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. COBURN (when his name was called). Present.

Mr. HATCH (when his name was called). Present.

Mr. INHOFE (when his named was called). Present.

Mr. KYL. The following Senators are necessarily absent: the Senator from New Hampshire (Ms. AYOTTE), the Senator from South Carolina (Mr. DEMINT), the Senator from South Carolina (Mr. GRAHAM), the Senator from Illinois (Mr. KIRK), the Senator from Utah (Mr. LEE), the Senator from Arizona (Mr. MCCAIN), and the Senator from Alaska (Ms. MURKOWSKI).

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

The yeas and nays resulted—yeas 56, nays 34, as follows:

[Rollcall Vote No. 186 Ex.]

YEAS—56

Akaka	Gillibrand	Nelson (NE)
Baucus	Hagan	Nelson (FL)
Begich	Harkin	Pryor
Bennet	Inouye	Reed
Bingaman	Johnson (SD)	Reid
Blumenthal	Kerry	Rockefeller
Boxer	Klobuchar	Sanders
Brown (MA)	Kohl	Schumer
Brown (OH)	Landrieu	Shaheen
Cantwell	Lautenberg	Snowe
Cardin	Leahy	Stabenow
Carper	Levin	Tester
Casey	Lieberman	Udall (CO)
Collins	Manchin	Udall (NM)
Conrad	McCaskill	Warner
Coons	Menendez	Webb
Durbin	Merkley	Whitehouse
Feinstein	Mikulski	Wyden
Franken	Murray	

NAYS—34

Alexander	Grassley	Portman
Barrasso	Heller	Risch
Blunt	Hoeven	Roberts
Boozman	Hutchison	Rubio
Burr	Isakson	Sessions
Chambliss	Johanns	Shelby
Coats	Johnson (WI)	Thune
Cochran	Kyl	Toomey
Corker	Lugar	Vitter
Cornyn	McConnell	Wicker
Crapo	Moran	
Enzi	Paul	

ANSWERED ''PRESENT''—3

Coburn	Hatch	Inhofe

NOT VOTING—7

Ayotte	Kirk	Murkowski
DeMint	Lee	
Graham	McCain	

The PRESIDING OFFICER. On this vote, the yeas are 56, the nays are 34, 3 Senators responded ''present.'' Three-fifths of the Senators duly chosen and sworn not having voted in the affirmative, the motion is rejected.

Mr. COBURN. We just disallowed one of the best candidates for the appellate court in my 8 years since I have been in the Senate. Magistrate Judge Bob Bacharach is a stellar individual rated ''very highly qualified'' by the American Bar Association. What has happened is we are in the position today because of games that are being played, political games.

Let me just put into the RECORD what is going on. There are three judges ahead of Bob Bacharach in line. We have had a Leahy-Thurmond rule for some 20 years. I have been quoted saying I think it is a stupid rule. But the background is that protecting the prerogative of the Senate is one of the most important things the majority leader can do.

What we have seen happen with the lack of agreement this last holiday season over the moving forward of judges and their approval was the unconstitutional usurpation of power by the President of the United States in the appointment, during our pro forma sessions, of four individuals, one to CFPB and three to the NLRB.

Quite frankly, if we look at what Madison wrote in Federalist 51:

> The great security against a gradual concentration of the several powers in the same branch of government consists in giving to those who administer each branch the necessary constitutional means and personal motives to resist encroachment of the others. Ambition must made to counteract ambition. The interest of the man must be connected with the constitutional rights of the place.

So started the saga in January of this past year, where the reaction of my colleagues on my side of the aisle was to shut down, in response to the President's move, all circuit court confirmations.

I stood in my caucus and fought that. I thought it was the wrong action then. I still think it would have been the wrong action. But I convinced my caucus not to go that direction. To do that, I agreed I would consent to the Leahy-Thurmond rule in this election cycle. But I hope this is the last election cycle we use the Leahy-Thurmond rule.

Because on the other side of the constitutional issues is that a duly elected President does have the right to have their nominees considered, whether I agree with them or not. To prove this, that this was a stunt rather than anything other than that, and Bob Bacharach becomes the pawn in that, is that we had an agreement on judges. Then we had cloture filed on fourteen district court judges, of which there was no real controversy.

All of those district court judges, after that cloture was filed on them and then withdrawn, have henceforth been approved. To the American public, the game is politics and not policy for our country. To me, it saddens me. It frustrates me that we are at this state because it is not a whole lot different than what we see in the playground at a kindergarten.

The person who most has spoken in favor of the Leahy-Thurmond rule is the chairman of the Judiciary Committee. Yet we find this impasse today. So what we ought to all do, every Member of the Senate and the Judiciary Committee during the break after this election, is work together to try to resolve this so this does not happen to any other President and does not do damage to the Senate and the integrity of the Senate and the game on judges. The President gets elected, with their home State Senators, they make a selection. We should not use the filibuster, unless a judge is highly questionable or biased in their viewpoint.

I regret that we are in this position. I think this was just a vote to delay Bob Bacharach's eventual confirmation. If President Obama wins the election, I fully expect Judge Bob Bacharach will be approved. If he does not win the election, I plan on standing and fighting for this judge for this same position under a Republican President because he is exactly what we want on a court, someone who is right down the middle in terms of what the law means, what the Constitution means. He has stellar intellectual capabilities, and he has the qualities we all would want, both from the right and the left, as a fair decider of the facts. That is what we want in judges. He will make an ideal appellate judge, regardless of his political affiliation.

If we cannot get there then what that says is the partisan politics of today, as everybody outside Washington recognizes, is killing our country.

LEGISLATIVE SESSION

The PRESIDING OFFICER. Under the previous order, the Senate will resume legislative session.

CYBERSECURITY ACT OF 2012

The PRESIDING OFFICER. Under the previous order, the motion to proceed to S. 3414 is agreed to and the clerk will report the measure.

The assistant legislative clerk read as follows:

> A bill (S. 3414) to enhance the security and resiliency of the cyber and communications infrastructure of the United States.

The PRESIDING OFFICER. The majority leader.

Mr. REID. Madam President, I ask unanimous consent that there now be a period of debate only on S. 3414, and that this will go forward until 2:15 p.m. on Tuesday, July 31; further, that at 2:15 p.m. on that date, Tuesday, I be recognized.

The PRESIDING OFFICER. Is there objection?

Mr. COBURN. Madam President, reserving the right to object.

The PRESIDING OFFICER. The Senator from Oklahoma.

Mr. COBURN. Just a question through the Chair to the majority leader. I had planned to make a statement on Judge Bacharach, and the Senator is saying we will have debate only. Will that preclude a unanimous consent for speaking as in morning business?

Mr. REID. The Senator can do that. It is totally appropriate.

Mr. COBURN. I thank the Senator.

I have no objection.

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

The Senator from New Hampshire.

Mrs. SHAHEEN. Madam President, if the majority leader is finished, I ask unanimous consent to speak as in morning business.

The PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

Mr. REID addressed the Chair.

The PRESIDING OFFICER. The majority leader.

Mr. REID. Madam President, if I could ask my friend to withhold for a brief moment.

Mrs. SHAHEEN. That is fine.

Mr. REID. It is my understanding that Senator COBURN has been waiting around for a while to talk.

The Senator is OK waiting?

Mr. COBURN. Yes.

Mr. REID. OK.

The PRESIDING OFFICER. The Senator from New Hampshire.

Mrs. SHAHEEN. Thank you, Madam President.

I come to the floor this evening to talk about an amendment I have filed to the Cybersecurity Act, S. 3414. This is the fourth time I have filed this amendment, and it is not on the Cybersecurity Act per se, although it does address energy use, which is one of the critical challenges we face as we are trying to address cybersecurity in this country.

This is an amendment that is the substance of S. 1000, the Energy Savings and Industrial Competitiveness Act, of which the other sponsor is Senator ROB PORTMAN, and he is a cosponsor on this amendment.

What the Energy Savings and Industrial Competitiveness Act and the amendment I filed does is create a national energy efficiency strategy for the United States. So this amendment is the same language Senator PORTMAN and I filed to the Bring Jobs Home Act and the Middle Class Tax Cut Act, and it is one we are going to continue to file because we think it is important for this amendment and this legislation to have an opportunity for a vote from this entire Senate because we think this is bipartisan legislation that has broad support among our colleagues.

This legislation is based on two important premises I have already spoken to in the Chamber: first, that the American public desperately wants Congress to work together in a bipartisan way to address this Nation's energy needs; and, second, that energy efficiency is the fastest, cheapest way to meet our energy challenges. Not only does it help us develop a strategy around energy, but it is a strategy that can be supported whether you live in New England, as I do, whether you live in the West, whether you live in the South. It is a strategy that is important whether you support fossil fuels—oil and gas—whether you support nuclear, or whether you support wind and solar. We all benefit from energy efficiency. It is also a strategy that creates thousands of good jobs.

There is evidence that the American public wants to see the Senate act on energy efficiency legislation. I think that evidence is overwhelming because last week I started an online campaign asking people to sign a petition calling on Senate leadership to bring this bill to the floor. The text of the petition is what we see here—small print so it is hard to read, but it asks people to support the Shaheen-Portman energy efficiency bill.

I just wish to read a section of it. It says:

> The Shaheen-Portman Act would help make the United States a global leader in the fastest and cheapest method we have for addressing our energy needs, energy efficiency. Energy efficiency is within our grasp. It uses proven technology that we can manufacture here at home to lower energy costs across all sectors of our economy.

In just a matter of days, we have already collected over 4,600 signatures from supporters across the country, and that number continues to grow. Anyone interested in signing the petition and in learning more about the many benefits of energy efficiency can easily do so by visiting my Web site at shaheen.senate.gov.

While drafting the bill, Senator PORTMAN and I met with a number of stakeholders so we could better understand the obstacles the private sector faces when they are trying to deploy energy-efficient technology. So we had discussions with people from energy-intensive companies, from trade groups, from those representing the real estate community, from environmental advocates and from financing organizations.

The feedback we received about ways to remove these barriers and drive the adoption of energy-efficient technologies became the basis for this legislation. As a result, we have a bill that provides a variety of low-cost tools that will speed this Nation's transition to a more energy-efficient economy.

The bill addresses three major areas of U.S. energy use: residential and commercial buildings, which consume 40 percent of all energy used in the country; the industrial sector, which consumes more energy than any other sector of the U.S. economy; and the Federal Government, which is the country's single biggest user of energy.

Highlights of the bill include: establishing advanced building codes for voluntary residential and commercial buildings to cut energy use. I would emphasize that those codes are voluntary. We worked with the real estate and the building industries on those codes.

Second, the legislation helps manufacturers finance and implement energy-efficient production technologies and practices because that is one of the biggest obstacles to retrofitting buildings for energy efficiency.

Third, the legislation would require the Federal Government to adopt better building standards and smart metering technology.

Our legislation is bipartisan. In addition to the thousands of signatures on this petition, it has support from well over 200 businesses, environmental groups, think tanks, and trade association. Those groups include: The National Association of Manufacturers, the U.S. Chamber of Commerce, the Environmental Defense Fund, businesses such as Johnson Controls, Honeywell, United Technologies Corporation.

This broad coalition of supporters recognizes that the legislation is an easy first step that will make our economy more competitive and our Nation more secure by reducing our dependence on foreign oil and still meeting the demand for energy saving technologies for individuals and businesses alike.

I think it is important to point out that there are real economic benefits. A recent study by policy experts at the American Council for an Energy-Efficient Economy found that the legislation will achieve savings for consumers and businesses. Specifically, their study found that by 2020, the bill could save consumers $4 billion a year once it is enacted. It would add 80,000 jobs to the economy.

In a time when we are worried about growing the economy, when we are worried about the fragile recovery, this is the kind of legislation that will allow us to create good jobs with off-the-shelf technologies. With the Shaheen-Portman energy efficiency bill, the Senate has an opportunity to provide the American people with exactly what they want, an effective bipartisan approach to addressing this Nation's energy needs that also creates jobs and grows the economy. I hope we will be able to persuade leadership and my colleagues that this is legislation that merits full debate and a vote on the floor and that we will be able to bring S. 1000 or this amendment to the floor for a vote.

I yield the floor.

The PRESIDING OFFICER. The Senator from Oklahoma.

Mr. COBURN. Madam President, I ask unanimous consent to speak as in morning business for such time as I may consume, and that when I finish, the Senator from Ohio be recognized for 10 minutes.

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

APOLOGY

Mr. COBURN. Madam President, I wished to come to the floor to talk about two or three subjects. The first is to issue an apology to the majority leader. I do not apologize for my frustration with this place, but occasionally my words are harsh and inaccurate. This past week, I used words that were inappropriate in describing his actions in the Senate, and for that I offer a public apology.

I do not apologize for how I think the Senate is being run and the damage that I think is being done to the country, but as an individual, he has a very difficult time and I understand that and to him I ask his forgiveness.

FISCAL CLIFF

Madam President, if I was coming to the floor with intelligence about an imminent threat to our national security, Americans would demand that our government and this body take immediate action. If an Army was on our border,

if missiles were about to be launched at our territory or if there were a terrorist plot in motion, doing anything less than us uniting in the face of that threat and taking decisive action would be seen as cowardice and foolishness.

Yet that is precisely where we are today, which brings me to my frustration with the majority leader. The threat, though, does not come from traditional armies or terrorists, the threat comes from our unsustainable spending and this body's refusal to unite and take action. It is not just the conservatives who are sounding the alarm, the warnings are coming from our military leaders, diplomats, and statesmen on both sides of the aisle, as well as the international financial community.

ADM Mike Mullen, the retired Chairman of the Joint Chiefs of Staff, while he was still Chairman, said the greatest threat to this Nation is its debt. We have done not one thing since January to address that problem. We are having spats over judges. We are having spats over all the small things. But the greatest imminent danger to our country, we are doing nothing about. I believe we have less than 2 to 5 years to act to make a significant change in our path.

No one knows when this Nation will cross the point of no return. We may have already. But there is a point where we will lose control of our own destiny. It is coming. The fact that the Senate, this year, has had fewer votes than at any time since 1947, according to the Congressional Research Service—why is that? Because we have a political year. We don't want to take votes. We don't want to have to explain to our constituencies why we voted yea or nay on something. So the whole goal is to not vote.

Ultimately, the whole goal is to not address the very pressing issues facing this country. What do you think is going to happen to the Defense Department with no Defense authorization bill? They are in la-la land. Where do they go? We are not going to give them the direction with which to spend the largest discretionary amount of money in our government—$600 billion. They are going to be coasting, flying by the seat of their pants. They are not going to have radar or anything. There is not going to be any stealth. Yet we refuse to do that.

We have spent a larger amount of time in quorum calls—37 percent of the time this year—nothing but quorum calls. Less than one-third an amount of the time available to the Senate has actually been on the business associated with the country, and most of the business we have addressed isn't this critical risk in front of our country.

Last week, Vanguard, the largest private owner of U.S. bonds—$186 billion they own of U.S. bonds—said we have until 2016 to act. If we don't act, we will go into a debt spiral. Bond investors will revolt, they will drive up prices—drive up interest rates and drop prices. We already know from CBO that the entitlement programs are on the brink of insolvency. Social Security disability—we have added 3.2 million people to those rolls since January 1, 2009. That system will be bankrupt in less than 18 months; 8½ million people depend on that. And there has not been a comment from the leadership in addressing a trust fund that will be out of money in less than 18 months.

Our Founders believed that republics that lived beyond their means don't survive. They talked about it. History is full of examples. Europe is reminding us of that today. The euro in Europe, as we know it, is on its deathbed. Every month, every week there is a new set of resuscitative efforts that are not working. What is the real problem? The real problem is they spent money they didn't have on things they didn't need.

If you want to see what America will look like in 2 or 3 years, just look at Europe. Look at the demonstrations, look at the crying out of the masses to say: How did we get here? The pain of fixing it is too great. That is why we should be addressing our problems now.

The reason America looks good is that we are the least wilted rose in the bud vase. The only reason we look good is because they look so bad. We are at 103 percent debt to GDP. It is costing us at least 1.2 million jobs in new job creation every year. We are at historical interest rates. Our interest costs per year would be over $1 trillion. The interest rates are falsely low because of what the Federal Reserve has done.

The price to pay for that is coming in the future. What is the contrast? I ask seniors all the time: Do you think we ought to save Medicare?

They say: Yes.

I say: Do you think we ought to save Medicare just like it is.

They say: Yes.

I say: If we save Medicare just like it is, do you know that your grandchildren will have a standard of living that will be one-third lower than yours was?

Then they say: No.

America is used to doing hard things. It is just that the Senate right now will not do the hard things, will not come together, will not make the sacrifices. We value our positions more than we value the country we live in. The consequences are showing.

We have an 8.2-percent unemployment rate. If we use the same statistics we used in 1980, our unemployment rate is above 9.6 percent—just measuring it the same way we did it 32 years ago. Now that we are measuring it differently, we don't see the real impact.

Today we are dangerously close to a global great depression. Let's remember the last time the world saw a great depression. That depression was a leading cause of the global war that killed 60 million people—2.5 percent of the world's population. Do we dare go down that path by putting politics ahead of principle and policy?

Fortunately, many of our leaders see this threat and are calling on us to take action. Consider this exchange between former Secretary of State James Baker and current Secretary of State Hillary Clinton last month on ''The Charlie Rose Show'':

Secretary Baker:

I know one thing. We are broke. We can't afford wars anymore. We can't afford a lot of things, and the biggest threat facing the country today is not some threat from the outside—Iran, nuclear weapons, or anything else—it's our economy. We better darn well get our economic house in order because the strength of our Nation has always depended upon our economy. You can't be strong politically, militarily, or diplomatically if you are not strong economically.

He is giving us a foreshadow of what is coming.

Secretary Clinton said this in response:

Well, amen to that, because I have had to go around the world the last 3½ years reassuring many leaders both in the governments and the business sectors of a lot of countries that the United States was moving forward economically, that we were not ceding our leadership position, and that we are as powerful as ever. But we recognized that we had to put our economic house in order.

If former Secretary Baker and Secretary Clinton can agree, why can't we? They both see the same thing. The only problem is we haven't put our economic house in order.

I know it is the Senate majority leader's position to try to protect both his incumbent President and his Members. I know that conventional wisdom says we cannot get anything done in an election year. But I want to tell you that isn't good enough anymore—not good enough for the country. The country deserves better.

By doing nothing, we are pushing our children and grandchildren off a fiscal cliff. By doing nothing, we are guaranteeing the very tax increases and cuts in entitlements that both sides say they want to avoid.

If you are an unemployed American right now or someone struggling to make ends meet, when is the right time for us to act? Is it a perfect political moment that is always a mirage beyond the horizon of the next election or is it today or this week? The American people have lost their confidence in us because we refuse to act even as we call on others to do things that we will not do ourselves.

Today we are asking our soldiers to risk their lives for our country. Why can't we do the same? Why are we allowed to play it safe when we ask others to make the ultimate sacrifice—especially when we as elected leaders have so much less at stake.

I believe the American people want us to do hard things and will actually reward us for demonstrating leadership and courage. The problems before us today can all be solved, but delay means the pain that comes with the solution is much greater. Yet to delay—

that is the path we have chosen in the Senate; that is the path the President has chosen—to not face the real issues, the coming and impending bankruptcy of Medicare, and the fact that the average Medicare couple will take three times more out of Medicare than what they put in, and the fact that the baby boom generation will overwhelm the trust fund that pays the hospital bills the worst-case scenario is that in 4 years the Medicare trust fund will be bankrupt. I know that sounds like a lot of things. Let me show the American people some examples.

We hear mindless, partisan rhetoric about which side is to blame, just like the debate we heard before the vote on Judge Bacharach. The truth is both sides are to blame, both Republicans and Democrats, when Republicans had the chance to restore limited government, and we helped double the size of government.

Meanwhile, the leaders today—their chief complaint is we didn't overspend enough. I know the Senate majority leader has a tough job and the burden of leadership, but he is refusing to accept the responsibility that is truly ours today. This Congress will be measured by our actions.

At the end of this week, for 5 weeks, the Senate is going to take off, and we are going to be just like Rome. Actually, what should happen to every Senator as we leave this place at the end of the week, we should each be handed a fiddle so we can all fiddle while the government and the financial situation and the economic chaos that is ours today grows unabated.

Real leadership isn't about being right, it is about doing the right thing. We are not doing the right thing in the Senate today. We are not reforming the Tax Code that is 90,000 pages and takes 110,000 IRS employees to administer. We are not addressing the impending bankruptcy of Medicare. We are not assuring the solvency of Social Security and increasing payments for those on the very low end of the totem pole. We are not addressing the key issues facing our country.

Why are we here if we are not going to address those issues? We are addressing every issue but those. Again, it is evident my frustration is high. I want the Senate to return to the body it was when I first came here. I think we can do that. I think Senator REID can lead us to do that. Every day we waste, every day we are not fixing the real problems, the disease that faces our country means we are responsible for a significant increase in the pain and disruption that is coming. Let it not be so.

I yield the floor.

The PRESIDING OFFICER. The Senator from Ohio is recognized.

OLYMPIC OMISSION

Mr. BROWN of Ohio. Madam President, I rise today because there was an obvious omission in the Olympic opening ceremony on Friday.

Forty years after 11 Israeli Olympians and a German police officer were murdered in the 1972 Munich games, the London games opened with no acknowledgement of this tragedy. There was neither mention nor a moment of silence for those victims of the Munich massacre.

Forty years ago, on September 4, five Palestinians stormed the apartments of the Israeli national team in the Olympic Village, murdering 11 Israeli team members. Yet, again and again, the IOC has rejected requests to hold a moment of silence for the Munich 11 at the opening ceremonies.

I thank Senator GILLIBRAND for her resolution calling on the IOC to hold a moment of silence at the opening ceremonies to remember the 1972 Munich massacre.

I remind the International Olympic Committee that it is not too late. We can still pay tribute to these Olympians. These athletes were not random victims. They were targeted because of the country they represented and the beliefs they held.

Jacques Rogge, the IOC President, has said:

> We feel that the opening ceremony is an atmosphere that is not fit to remember such a tragic incident.

That is the best he can do.

On the 40th anniversary, I cannot think of a more appropriate moment to remember and honor these 11 Olympians.

The Munich massacre is part of the Olympic story. We can't erase it, and we should not overlook it. After all, we know what happens when we avoid the past. Of course, we cannot afford to repeat it.

I ask we all do everything we can to convince the IOC to step up and do the right thing.

Let me explain why this especially matters for people in my home State of Ohio—in greater Cleveland, the part of Ohio which I call home. In Beachwood, OH, a suburb east of Cleveland, there is a national memorial to David Berger, an American citizen and one of the 11 Israeli team members killed in Munich.

As a Nation, we honor his memory and the memory of his Israeli teammates, but we also have a moral responsibility to hold accountable those responsible for his death. Holding them responsible includes those who supported and financed the terrorists who perpetrated these actions.

We had the chance to hold Libya accountable. Yet during negotiations that led to the 2008 U.S.-Libya claims settlement agreement, Mr. Berger was not included, despite widely accepted evidence that Libya played an important role in the massacre.

We know the Qadhafi regime financially supported terrorist groups such as the Black September organization. It supported them and it welcomed the bodies of the dead terrorists from the Munich massacre back to a hero's tribute.

Seeking justice and compensation for victims of global terrorism sends a powerful message to those who may be seeking to do further harm. The window of opportunity to engage the new Libyan Government has never been greater. Libyan Ambassador Ali Suleiman Aujali said earlier this month in an op-ed in the Washington Post that he hopes ''that Washington considers an enterprise fund for Libya'' and that ''we would work closely with the U.S. Government on its creation.''

Those are the words of the Libyan Ambassador. Such a fund should include all those who deserve restitution for the losses they suffered. This includes the Berger family.

This is about letting violent extremists know they and their supporters will be pursued until justice is served—sending a clear signal to those contemplating terrorism as a political tool.

As we all cheer on the American athletes in the next couple of weeks, I ask that we all take a moment to think about the Munich massacre, about David Berger, and about what more we can do to preserve their legacy and resolve to thwart those who by their use of terror and violence would undermine all that the Olympic games are supposed to represent.

Madam President, 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. BROWN of Ohio. Madam 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. BROWN of Ohio. Madam President, I ask unanimous consent that the Senate proceed to a period of morning business, with Senators permitted to speak therein up to 10 minutes each.

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

REMEMBERING REPRESENTATIVE DEWAYNE BUNCH

Mr. MCCONNELL. Madam President, with sadness I rise today to mark the passing on July 11, 2012, of former Kentucky State Representative Dewayne Bunch. As a teacher and State representative, Dewayne served the people of the Commonwealth, especially those in Whitley and Laurel Counties, with distinction. He also proudly served our country in Iraq as a member of the Kentucky National Guard. Elaine and I send our condolences to his wife Regina, his family, his many friends, and all those at Whitley County High School who knew and loved him.

A Corbin resident, Representative Bunch died at age 50. He is survived by his wife Representative Regina Bunch, and he was the father of three daughters. Though his life was cut short, it was characterized by a dedication to serving others in his community, State, and country. Representative

Bunch was a member of the Kentucky National Guard for 23 years, where he notably led the Mountain Warriors in Iraq as a first sergeant.

Although he valiantly represented his Nation and State abroad, Representative Bunch also did much of his work from within the community. He was a math and science teacher at Whitley County High School for 17 years, and in 2010, with the support of the citizens of the 82nd District, was elected State Representative. However, after an injury in 2011, Bunch resigned from his post to receive medical treatment. His wife Regina ran for the position and succeeded her husband as the 82nd District's representative.

The loss of Representative Bunch to the members of the Whitley County community is immeasurable, and Dewayne's death has saddened Kentuckians across the State. Members of the State House Republican Caucus said he was committed to serving the public and ran for elected office in order to more fully serve the people of the Corbin community. The Governor of the State of Kentucky, Steve Beshear, acknowledged the loss of Representative Bunch by ordering flags lowered to half-staff.

Hundreds of people came to pay their respects at Representative Bunch's funeral on July 15, held at Highland Park Cemetery in Williamsburg. Military graveside honors were conducted by the Kentucky National Guard. At the funeral, Representative Bunch was posthumously awarded the Kentucky Distinguished Service Medal to commemorate his work on behalf of his community and the State of Kentucky. I am privileged today to recognize Representative Bunch and his legacy of service to the Commonwealth.

Madam President, at this time I ask my colleagues in the U.S. Senate to join me in honoring the life of Representative Dewayne Bunch of Corbin, KY. The Croley Funeral Home has published an obituary that highlighted his achievements and pays tribute to those Representative Bunch leaves behind. I ask unanimous consent that said article be printed in the RECORD.

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

[From the Croley Funeral Home, July 12, 2012]

DEWAYNE EVERETT BUNCH

Dewayne Everett Bunch of Old Corbin Pike, Williamsburg, Kentucky, departed this life on Wednesday, July 11, 2012, at the Oak Tree Hospital in Corbin, Kentucky. He was 50 years, 4 months, and 20 days of age. He was born on February 22, 1962, in Whitley County, Kentucky, to Charles Everett Bunch and the late Gloria Eunice (Rains) Bunch. He was a member of Highland Park Baptist Church. Dewayne was a veteran of the United States Army and retired from the Kentucky National Guard after 24 years of service. He was a member of the Kentucky House of Representatives (82nd District) and a schoolteacher at the Whitley County Schools for over 17 years.

He is survived by wife Regina Petrey Bunch of Williamsburg, Kentucky; three daughters, Stephanie Fox (Brad) of Lexington, Kentucky, Kristen Bowlin (Tommy), and Brittany Morgan (Jeremiah) all of Williamsburg, Kentucky; two grandchildren, Miah Morgan and Thomas Blake Bowlin; his father, Charles Everett Bunch of Williamsburg, Kentucky; a sister, Shanda Weddle (Bruce) of Williamsburg, Kentucky; brothers, Tim Bunch (Lisa) and Jim Bunch, all of Williamsburg, Kentucky; his father and mother-in-law, Herbert and Teresa Petrey of Williamsburg, Kentucky; several nieces and nephews; and a host of other relatives and friends to mourn his passing.

Visitation will be from 12:00 noon until the funeral hour on Sunday, July 15, 2012, at Croley Funeral Home.

The Funeral Service will be at 4:00 P.M. Sunday, July 15, 2012, at the Croley Funeral Home Chapel with Rev. Doyle Lester and Rev. Gerald Mullins officiating. A Masonic Service will be conducted at 4:00 P.M. by the Williamsburg Masonic Lodge #490 F&AM. He will be laid to rest in the Croley Addition of Highland Park Cemetery in Williamsburg. Military Graveside Honors will be conducted by the Kentucky National Guard. Dan Ballou, Gary Taylor, Terry Huddleston, Bear Lancaster, J.R. Peace, James York, Danny Ford, Bobby Freeman, Tom Cline, and Alex Patrick will serve as pallbearers. Honorary Pallbearers will be the Citizens of the 82nd District.

In lieu of flowers, memorials may be made to the Dewayne Bunch Scholarship Fund at Forcht Bank of Williamsburg and Corbin.

RECENT EVENTS IN EL SALVADOR

Mr. LEAHY. Madam President, I want to speak very briefly about recent events in El Salvador which is in the midst of a constitutional and political crisis involving the composition and power of the Supreme Court.

Essentially what happened is that in June the Supreme Court ruled that the National Assembly had abused its power by naming justices to the court on two separate occasions, and ordered a new judicial selection process with which the National Assembly then refused to comply. A majority of the deputies took the extraordinary step of appealing the Supreme Court's decision to the Central American Court of Justice, and a final ruling is expected in a matter of days.

Last week, Congressman JIM MCGOVERN, who is probably more knowledgeable about El Salvador than anyone else in Congress, and I commented on the situation. We said:

We are encouraged by the commitment by President Funes and representatives of El Salvador's political parties to resolve this crisis expeditiously. We agree with the Department of State that this is a matter to be resolved by Salvadorans through dialogue, and we reaffirm our support for U.S. assistance for El Salvador which addresses a range of mutual interests, from improving law enforcement to combating poverty.

Over the past 30 years, El Salvador has faced many challenges, from civil war, to corruption, to cyclones. This constitutional political crisis is the latest test of whether the country's governmental institutions can emerge stronger, the rule of law strengthened, and its people more united.

Since then, there has been further progress towards a resolution of this crisis. As a former prosecutor, Chairman of the Judiciary Committee and Chairman of the Appropriations Subcommittee on State and Foreign Operations that funds international aid programs, I can think of few things as important to any society as an independent judiciary. Like free and fair elections, it is a cornerstone of democratic government. Sometimes I agree with the decisions of our Supreme Court and sometimes I disagree. But we comply with its decisions because we know the alternative is chaos and the erosion of the checks and balances that protect our 226 year old democracy.

I suspect the people of El Salvador feel similarly, and I am hopeful that however their representatives resolve this matter the independence of the Salvadoran judiciary will be preserved and strengthened.

LIFTING OF OBJECTION

Mr. GRASSLEY. Madam President, on June 27, I provided notice of my intent to object to proceeding to the nominations of Mark J. Mazur, to be an Assistant Secretary of the Treasury, and Matthew S. Rutherford, to be an Assistant Secretary of the Treasury. My support for the final confirmation of these nominees depended on receiving information from both the Treasury Department and the Internal Revenue Service regarding their implementation of the tax whistleblower program. Since I have received the responses, I no longer object to proceeding to these nominations.

The IRS is making progress in paying whistleblower awards under the old statute over 90 awards paid from October 1, 2011, until now. However, I want to make clear that the responses do not alleviate my concerns about these agencies' implementation of changes to the tax whistleblower statute I authored almost 6 years ago. Regulations to implement the new reward program have yet to be issued and only a handful of awards are expected to be paid out before the end of this year.

I began asking questions about the program's implementation in 2010. I wrote again in 2011 and then again on April 30 of this year. Unfortunately, I did not get complete answers until I objected to proceeding to the nominations of Mr. Mazur and Mr. Rutherford.

If I hadn't objected to proceeding to these nominations, Congress would not have received the most recent annual report on the whistleblower program that is mandated by law. It was provided to Congress on June 13, 2012, for the fiscal year ended September 30, 2011. That is almost 9 months from the end of the year for which it contains data.

If I hadn't objected to proceeding to these nominations, the IRS likely would not have acknowledged that there is, in fact, a problem with timely processing whistleblower claims. IRS Deputy Commissioner Miller's June 20, 2012, directive to IRS executives and

senior managers is a good first step toward correcting this problem.

However, more needs to be done. IRS still has not committed to prioritizing claims raised by whistleblowers. In addition, the important protections afforded to taxpayers, including the right to appeal IRS decisions, delay IRS from actually collecting the taxes for years and, as the law is currently written, the taxes must be collected first before a whistleblower can be paid any money.

From my long history of oversight of the IRS, I know that it is essential that taxpayers be protected from sometimes overeager IRS employees. Yet there must be a way to ensure that the process and procedures that exist to protect taxpayers don't deter whistleblowers from coming forward. The Treasury Department and the IRS have agreed to participate in a roundtable discussion that I hope will help identify solutions.

It is unfortunate that objecting to these nominees, both of whom were approved by the Finance Committee by unanimous, bipartisan votes, was the only way I could get information about the whistleblower program. At least there is now more information than ever before about the IRS whistleblower program.

BULGARIA TERRORIST ATTACKS

Mr. CARDIN. Madam President, I rise to express my outrage at the recent attack on a tour bus in Burgas, Bulgaria, that killed five Israeli citizens and the Bulgarian driver and injured scores of passengers. This heinous act was obviously the handiwork of terrorists who prey on innocent civilians in order to shock and horrify the world and try to rally some to a twisted, violent ideology. The terrorists must be stopped.

I am equally outraged by the fact that the Burgas attack appears to be the latest in a series of attacks on Israeli citizens. There have been several since the beginning of this year alone, two aimed at Israeli diplomats in India and Georgia in February, as well as a foiled plot against tourists in Cyprus the week before the tragedy in Burgas. The attacks targeting Israeli Embassy personnel in India and Georgia fell on the 18th anniversary of a suicide bombing of the Jewish Community Center in Buenos Aires which killed 85 people. Argentine authorities blamed that attack on Hezbollah operatives.

All of these attacks have the hallmarks of Iranian involvement or plots by their surrogates. The day after the attacks in India and Georgia, Iranian nationals involved in a bomb-making plot in Thailand were arrested after they accidentally detonated their homemade explosives, severely injuring one of the perpetrators. Thai officials reported that the improvised explosives found in Bangkok were the same as those used in India and Georgia.

I understand that the investigation of the Burgas attack is ongoing and the United States and other countries are working closely with Bulgarian officials. White House counterterrorism chief John Brenan has visited Bulgaria, and, while he did not implicate Iran or Hezbollah in public statements he made while there, he pointed out that both Tehran and its Lebanese surrogate have been implicated in attacks on civilians in the past.

Israeli Prime Minister Benjamin Netanyahu has stated that Israel has ''fully substantiated intelligence'' that the Burgas attack was carried out by Hezbollah. I have not seen that information, but I think that based solely on press reports of results thus far in the investigations of these attacks, one can reasonably conclude that Iran and Hezbollah have been involved—further evidence of Iran's longstanding use of political violence and sponsorship of terrorism to achieve its goals.

According to a recent edition of the Jewish Press, the Director of Israel's Mossad and the Chief of its Shin Bet have said that Iran and Hezbollah have tried to commit terrorist attacks against Israeli diplomats, businessmen and tourists in over 20 countries during the past 2 years.

We must stand with the people and the Government of Israel. We must lead the international community in redoubling efforts to assist Israel, and all countries on whose soil these heinous acts are committed, in tracking down the terrorists and bringing them to justice and continue to work to prevent such attacks in the future.

I am confident that my colleagues on both sides of the aisle support our government's work with Israel and the international community to counter Iran's insidious network of terror.

REMEMBERING NEIL McMURRY

Mr. BARRASSO. Madam President, Wyoming has experienced an incredible loss. I rise today to remember one of Wyoming's most beloved citizens, Neil McMurry. On Thursday, July 19, 2012, Neil passed away at the age of 88. During his remarkable life, Neil made a profound and lasting contribution to the Casper community and the great State of Wyoming.

Neil was a successful entrepreneur, a committed citizen, and a good friend. Throughout his life, Neil always demonstrated an enduring commitment to his family, Wyoming, and our Nation. He loved his family. He loved his home State of Wyoming. He loved his country.

Ann Chambers Noble, a Wyoming author, recently wrote Neil's biography, ''Hurry McMurry: W.N. 'Neil' McMurry, Wyoming Entrepreneur.'' The title appropriately describes this extraordinary man. He grew up during the Great Depression, and saw firsthand the impact it had on his community. In 1941, Neil joined the U.S. Army Air Corps. He flew over 29 missions in Europe as a turret gunner on a B–17 aircraft during World War II.

Following his brave service to our Nation, Neil returned to Wyoming to raise a family and start a very successful business career. Neil was a man with determination, integrity, and a strong work ethic. He recognized the vast opportunities and great potential Wyoming has to offer. In 1949, he saw opportunity in constructing roads and highways across Wyoming. Along with his business partner, Vern Rissler, the Rissler-McMurry Company became one of the largest highway construction companies in Wyoming. The company built much of Wyoming's transportation routes.

While many people would have retired after running a successful contracting firm for over three decades, Neil was on the lookout for new opportunities. Neil and his business partners, John Martin and Mick McMurry, had a hunch that significant natural gas was in the Jonah Field in southwest Wyoming. In 1991, the McMurry Oil Company purchased wells and mineral leases in the Jonah area. His vision and willingness to take a risk turned into a natural gas play of historic proportions.

Neil McMurry will be remembered for his successful business endeavors that created thousands of jobs for the people in Wyoming. His efforts and entrepreneurial spirit significantly impacted Wyoming's economy.

While his business abilities will continue to be admired, it will be his selfless devotion to others and his willingness to give back to his community that will forever keep his memory in the hearts of the people of Wyoming. His charitable donations made a difference in the lives of people in his community.

Even though he lived a long life, Neil left us too soon. His remarkable contributions to the youth of Wyoming will be honored on August 7 by the Boys and Girls Clubs of Central Wyoming. While this would have been just one of many honors, it was very special to Neil. Through the generosity of the McMurry Foundation, Neil and his family have given unprecedented levels of support to Wyoming organizations particularly organizations supporting our youth.

My wife Bobbi and I will truly miss him. We are blessed that Neil was our friend and grateful for the moments we spent together. During this time of such great loss, we find solace in knowing that the legacy of Neil McMurry will live on.

Bobbi and I extend our deepest sympathy to the McMurry family. We wish his family all of our best and send our prayers to each of them.

ADDITIONAL STATEMENTS

MELBA, IDAHO

● Mr. RISCH. Mr. President, today I wish to congratulate and acknowledge

the 100th anniversary of the founding of the city of Melba, Idaho. Starting August 17, 2012, the citizens of Melba will gather throughout the weekend to commemorate this special time in their southwestern Idaho community.

Melba was founded by Clayton C. Todd, naming the yet-to-be town after his 4-year-old daughter. Stopping in Idaho on his way to Alaska to mine for gold, Mr. Todd heard about a State land sale. He purchased 160 acres of land and laid out the town site. He had done his homework and saw that this land with a siding on the railroad and expanding farms throughout the area would cut five miles off the route to the nearest town of Nampa and the mainline railroad.

Melba became a small boom town in the middle of an agricultural area. Shortly after World War I, the area became famous for its sweet corn seed. Area farmers expanded their seed operations to grow carrot, onion and alfalfa seed, along with the corn. The rich, fertile soil, abundant water and the hot summer days with cool nights earned Melba the moniker ''The Seed Heart of America.''

Like many small communities in our great country, they have seen times of struggle. In 1949, Melba was hit hard by an epidemic of infantile paralysis, also known as polio. The residents not only supported one another, in 1950 they held the first Polio Auction, raising $2,000 for medical research on the disease. Now called the Melba Community Auction, area residents continue the tradition of helping one another as they raise funds for nonprofit organizations that provide services to those in and around Melba.

The spirit of small town America is alive and well in Melba. They believe in helping their neighbors as well as strangers. Their schools are a source of pride and strongly supported by the community. And as to their Fourth of July celebration? Let me put it this way—no one can question their patriotism and love of America! Theirs is a grand celebration of our Nation's birthday.

So, Madam President, I am very proud to recognize this landmark anniversary and congratulate the community of Melba for this centennial. Melba has much to celebrate as well as to look forward to in its next century.●

TRIBUTE TO REX E. KIRKSEY

● Mr. UDALL of New Mexico. Madam President, I, on behalf of my colleague Senator BINGAMAN and myself, wish to recognize Rex E. Kirksey on the occasion of his retirement, following a distinguished career serving the agricultural community in our home State of New Mexico and elsewhere.

Mr. Kirksey has dedicated 32 years of his life working for New Mexico State University to improve agricultural outreach and to facilitate vital research. As the Superintendent of the NMSU Agricultural Science Center in Tucumcari, NM, Mr. Kirksey oversaw research programs focusing on developing forage and grazing systems for irrigated lands in New Mexico and the western United States.

In 2003, he took on additional responsibilities as superintendent of the Agricultural Science Center in Clovis, NM. Under his leadership, that institution emerged as the State's leading off-campus center with nationally and internationally recognized programs in agronomy, dairy management, peanut breeding, and crop stress physiology.

During his tenure at New Mexico State University, Mr. Kirksey authored many professional publications, including peer reviewed journal articles, proceedings papers, research reports and bulletins, progress reports and published abstracts, and an extensive range of business reports and correspondence. He has also given numerous presentations to industry and peer groups.

In addition to his work domestically, Mr. Kirksey has been involved with the Afghanistan Water, Agriculture, and Technology Transfer, AWATT, project—a partnership with USAID and New Mexico State University. This project aims to improve the community and farm-level management of the supply and demand of irrigation water resources for increased agricultural productivity and food security in Afghanistan. He also has worked with the Botswana Sustainable Agriculture Initiative, an international consortium with a goal to develop an integrated, sustainable agricultural system. The Botswana Initiative will assist both small and large farms to employ conservation agriculture practices to increase fresh water availability, grow more nutritious food, build agricultural infrastructure, create more agricultural jobs, and stimulate enterprise creation in rural areas.

Mr. Kirksey's leadership and expertise has made a difference in the lives of so many people in our Nation, as well as other parts of the world. Senator BINGAMAN and I thank Mr. Kirksey for his commitment and dedication to the people of New Mexico and to our agricultural communities. We would also like to thank his wife Cyndie and their three children for always supporting Rex in his endeavors. Thanks to his work and the work of our land grant institutions, farmers and ranchers across the country have access to the resources they need to help ensure our country's future competitiveness in an increasingly global economy.

We wish Mr. Kirksey continued success, and a most happy retirement.●

MESSAGE FROM THE HOUSE

At 2:28 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 bill, in which it requests the concurrence of the Senate:

H.R. 4078. An act to provide that no agency may take any significant regulatory action until the unemployment rate is equal to or less than 6.0 percent.

MEASURES PLACED ON THE CALENDAR

The following bill was read the second time, and placed on the calendar:

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.

MEASURES READ THE FIRST TIME

The following bills were read the first time:

H.R. 4078. An act to provide that no agency may take any significant regulatory action until the unemployment rate is equal to or less than 6.0 percent.

S. 3457. A bill to require the Secretary of Veterans Affairs to establish a veterans jobs corps, 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–7004. A communication from the Director of Congressional Affairs, Nuclear Regulatory Commission, transmitting, pursuant to law, the report of a rule entitled ''Requirements for Distribution of Byproduct Material'' ((RIN3150–AH91) (NRC–2008–0338)) received in the Office of the President of the Senate on July 24, 2012; to the Committee on Environment and Public Works.

EC–7005. A communication from the Director of Congressional Affairs, Nuclear Regulatory Commission, transmitting, pursuant to law, the report of a rule entitled ''NRC Regulatory Issue Summary 2012–08: Developing Inservice Testing and Inservice Inspection Programs Under 10 CFR Part 52'' (RIS 2012–08) received in the Office of the President of the Senate on July 24, 2012; to the Committee on Environment and Public Works.

EC–7006. 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; South Carolina 110(a)(1) and (2) Infrastructure Requirements for the 1997 and 2006 Fine Particulate Matter National Ambient Air Quality Standards'' (FRL No. 9705–8) received in the Office of the President of the Senate on July 25, 2012; to the Committee on Environment and Public Works.

EC–7007. 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: Prevention of Significant Deterioration and Nonattainment New Source Review; Fine Particulate Matter (PM2.5)'' (FRL No. 9704–7) received in

the Office of the President of the Senate on July 25, 2012; to the Committee on Environment and Public Works.

EC–7008. A communication from the Director of the Regulatory Management Division, Environmental Protection Agency, transmitting, pursuant to law, the report of a rule entitled ''Method 16C for the Determination of Total Reduced Sulfur Emissions From Stationary Sources'' (FRL No. 9701–9) received in the Office of the President of the Senate on July 25, 2012; to the Committee on Environment and Public Works.

EC–7009. 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; Florida; Sections 128 and 110(a)(1) and (2) Infrastructure Requirements for the 1997 8-Hour Ozone National Ambient Air Quality Standards'' (FRL No. 9705–2) received in the Office of the President of the Senate on July 25, 2012; to the Committee on Environment and Public Works.

EC–7010. A communication from the Director of the Regulatory Management Division, Environmental Protection Agency, transmitting, pursuant to law, the report of a rule entitled ''National Pollutant Discharge Elimination System Permit Regulation for Concentrated Animal Feeding Operations: Removal of Vacated Elements in Response to the 2011 Decision of the U.S. Court of Appeals for the Fifth Circuit'' (FRL No. 9705–6) received in the Office of the President of the Senate on July 25, 2012; to the Committee on Environment and Public Works.

EC–7011. 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; Control of Iron and Steel Production Installations; Sintering Plants'' (FRL No. 9702–6) received in the Office of the President of the Senate on July 25, 2012; to the Committee on Environment and Public Works.

EC–7012. A communication from the Assistant Secretary of the Army (Civil Works), transmitting, pursuant to law, a report relative to the Locks and Dam 52 and 53 Replacement Project (Olmsted Locks and Dam), Illinois and Kentucky; to the Committee on Environment and Public Works.

EC–7013. A communication from the United States Trade Representative, Executive Office of the President, transmitting a report relative to the inclusion of Canada in the ongoing negotiations of the Trans-Pacific Partnership (TPP) Agreement; to the Committee on Finance.

EC–7014. 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 ''Reallocation of Section 48A Credits under the Qualifying Advanced Coal Project Program'' (Notice 2012–51) received in the Office of the President of the Senate on July 24, 2012; to the Committee on Finance.

EC–7015. 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 ''Applicable Federal Rates—August 2012'' (Rev. Rul. 2012–21) received in the Office of the President of the Senate on July 24, 2012; to the Committee on Finance.

EC–7016. A communication from the Director, Office of Regulations, Social Security Administration, transmitting, pursuant to law, the report of a rule entitled ''Expedited Vocational Assessment Under the Sequential Evaluation Process'' (RIN0960–AH26) received in the Office of the President of the Senate on July 24, 2012; to the Committee on Finance.

EC–7017. A communication from the Director, Office of Regulations, Social Security Administration, transmitting, pursuant to law, the report of a rule entitled ''Regulations Regarding Income-Related Monthly Adjustment Amounts to Medicare Beneficiaries' Prescription Drug Coverage Premiums'' (RIN0960–AH22) received in the Office of the President of the Senate on July 24, 2012; to the Committee on Finance.

EC–7018. A communication from the Program Manager, Centers for Medicare and Medicaid Services, Department of Health and Human Services, transmitting, pursuant to law, the report of a rule entitled ''Medicare Program; Hospice Wage Index for Fiscal Year 2013'' (CMS–1434–N) received in the Office of the President of the Senate on July 25, 2012; to the Committee on Finance.

EC–7019. A communication from the Acting Inspector General, Office of Inspector General, U.S. Agency for International Development (USAID), transmitting, pursuant to law, the Office of Inspector General's (OIG) strategic plan for 2012–2016; to the Committee on Foreign Relations.

EC–7020. A communication from the Executive Analyst (Political), Department of Health and Human Services, transmitting, pursuant to law, the report of a vacancy in the position of Assistant Secretary for Public Affairs, Department of Health and Human Services, received in the Office of the President of the Senate on July 25, 2012; to the Committee on Health, Education, Labor, and Pensions.

EC–7021. A communication from the Chief Human Capital Officer, Corporation for National and Community Service, transmitting, pursuant to law, a report relative to a vacancy in the position of Inspector General, Corporation for National and Community Service, received in the Office of the President of the Senate on July 25, 2012; to the Committee on Health, Education, Labor, and Pensions.

EC–7022. A communication from the Chairman of the Council of the District of Columbia, transmitting, pursuant to law, a report on D.C. Act 19–397, ''Saving D.C. Homes from Foreclosure Enhanced Temporary Amendment Act of 2012''; to the Committee on Homeland Security and Governmental Affairs.

EC–7023. A communication from the Chairman of the Council of the District of Columbia, transmitting, pursuant to law, a report on D.C. Act 19–396, ''Fiscal Year 2012 Second Revised Budget Request Temporary Amendment Act of 2012''; to the Committee on Homeland Security and Governmental Affairs.

EC–7024. A communication from the Chairman of the Council of the District of Columbia, transmitting, pursuant to law, a report on D.C. Act 19–398, ''Social E-Commerce Job Creation Tax Incentive Act of 2012''; to the Committee on Homeland Security and Governmental Affairs.

REPORTS OF COMMITTEES

The following reports of committees were submitted:

By Mrs. FEINSTEIN, from the Select Committee on Intelligence, without amendment:

S. 3454. A bill to authorize appropriations for fiscal year 2013 for intelligence and intelligence-related activities of the United States Government and the Office of the Director of National Intelligence, the Central Intelligence Agency Retirement and Disability System, and for other purposes (Rept. No. 112–192).

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 Mrs. FEINSTEIN:

S. 3454. A bill to authorize appropriations for fiscal year 2013 for intelligence and intelligence-related activities of the United States Government and the Office of the Director of National Intelligence, the Central Intelligence Agency Retirement and Disability System, and for other purposes; from the Select Committee on Intelligence; placed on the calendar.

By Mr. WARNER (for himself and Mr. JOHNSON of Wisconsin):

S. 3455. A bill to require the establishment of customer service standards for Federal agencies; to the Committee on Homeland Security and Governmental Affairs.

By Mr. BLUMENTHAL (for himself, Mr. WHITEHOUSE, and Mr. CORNYN):

S. 3456. A bill to amend title 18, United States Code, with respect to child pornography and child exploitation offenses; to the Committee on the Judiciary.

By Mr. NELSON of Florida (for himself and Mrs. MURRAY):

S. 3457. A bill to require the Secretary of Veterans Affairs to establish a veterans jobs corps, and for other purposes; read the first time.

By Mr. LAUTENBERG (for himself and Mrs. FEINSTEIN):

S. 3458. A bill to require face to face purchases of ammunition, to require licensing of ammunition dealers, and to require reporting regarding bulk purchases of ammunition; to the Committee on the Judiciary.

SUBMISSION OF CONCURRENT AND SENATE RESOLUTIONS

The following concurrent resolutions and Senate resolutions were read, and referred (or acted upon), as indicated:

By Mr. MERKLEY (for himself, Mr. CRAPO, Mr. CASEY, Mr. BLUMENTHAL, Mrs. MURRAY, Mr. BROWN of Ohio, Mr. AKAKA, and Mr. KOHL):

S. Res. 533. A resolution designating October 2012 as ''National Work and Family Month''; considered and agreed to.

ADDITIONAL COSPONSORS

S. 33

At the request of Mr. LIEBERMAN, the name of the Senator from New York (Mr. SCHUMER) was added as a cosponsor of S. 33, a bill to designate a portion of the Arctic National Wildlife Refuge as wilderness.

S. 438

At the request of Ms. STABENOW, the name of the Senator from California (Mrs. FEINSTEIN) was added as a cosponsor of S. 438, a bill to amend the Public Health Service Act to improve women's health by prevention, diagnosis, and treatment of heart disease, stroke, and other cardiovascular diseases in women.

S. 534

At the request of Mr. KERRY, the name of the Senator from Georgia (Mr. ISAKSON) was added as a cosponsor of S. 534, a bill to amend the Internal Revenue Code of 1986 to provide a reduced

rate of excise tax on beer produced domestically by certain small producers.

S. 752

At the request of Mrs. FEINSTEIN, the name of the Senator from Louisiana (Ms. LANDRIEU) was added as a cosponsor of S. 752, a bill to establish a comprehensive interagency response to reduce lung cancer mortality in a timely manner.

S. 845

At the request of Mr. ENZI, the name of the Senator from Georgia (Mr. ISAKSON) was added as a cosponsor of S. 845, a bill to amend the Internal Revenue Code of 1986 to provide for the logical flow of return information between partnerships, corporations, trusts, estates, and individuals to better enable each party to submit timely, accurate returns and reduce the need for extended and amended returns, to provide for modified due dates by regulation, and to conform the automatic corporate extension period to longstanding regulatory rule.

S. 1755

At the request of Mr. TESTER, the name of the Senator from Massachusetts (Mr. KERRY) was added as a cosponsor of S. 1755, a bill to amend title 38, United States Code, to provide for coverage under the beneficiary travel program of the Department of Veterans Affairs of certain disabled veterans for travel for certain special disabilities rehabilitation, and for other purposes.

S. 1843

At the request of Mr. ISAKSON, the name of the Senator from Alabama (Mr. SESSIONS) was added as a cosponsor of S. 1843, a bill to amend the National Labor Relations Act to provide for appropriate designation of collective bargaining units.

S. 1935

At the request of Mrs. HAGAN, the name of the Senator from Florida (Mr. NELSON) was added as a cosponsor 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.

At the request of Ms. COLLINS, the name of the Senator from Iowa (Mr. GRASSLEY) was added as a cosponsor of S. 1935, supra.

S. 1956

At the request of Mr. THUNE, the name of the Senator from North Carolina (Mrs. HAGAN) was added as a cosponsor of S. 1956, a bill to prohibit operators of civil aircraft of the United States from participating in the European Union's emissions trading scheme, and for other purposes.

S. 1979

At the request of Mr. CONRAD, the name of the Senator from Alaska (Mr. BEGICH) was added as a cosponsor of S. 1979, a bill to provide incentives to physicians to practice in rural and medically underserved communities and for other purposes.

S. 1990

At the request of Mr. LIEBERMAN, the names of the Senator from West Virginia (Mr. ROCKEFELLER) and the Senator from California (Mrs. BOXER) were added as cosponsors of S. 1990, a bill to require the Transportation Security Administration to comply with the Uniformed Services Employment and Reemployment Rights Act.

S. 1993

At the request of Mr. NELSON of Florida, the names of the Senator from Michigan (Mr. LEVIN) and the Senator from Vermont (Mr. SANDERS) were added as cosponsors of S. 1993, a bill to posthumously award a Congressional Gold Medal to Lena Horne in recognition of her achievements and contributions to American culture and the civil rights movement.

S. 2010

At the request of Mr. KERRY, the name of the Senator from Michigan (Ms. STABENOW) was added as a cosponsor of S. 2010, a bill to amend title II of the Social Security Act to repeal the Government pension offset and windfall elimination provisions.

S. 2264

At the request of Mr. HOEVEN, the name of the Senator from Arkansas (Mr. BOOZMAN) was added as a cosponsor of S. 2264, a bill to provide liability protection for claims based on the design, manufacture, sale, offer for sale, introduction into commerce, or use of certain fuels and fuel additives, and for other purposes.

S. 2347

At the request of Mr. CARDIN, the name of the Senator from Oregon (Mr. WYDEN) was added as a cosponsor of S. 2347, a bill to amend title XVIII of the Social Security Act to ensure the continued access of Medicare beneficiaries to diagnostic imaging services.

At the request of Ms. CANTWELL, the name of the Senator from Massachusetts (Mr. KERRY) was added as a cosponsor of S. 2347, supra.

S. 2472

At the request of Mr. CASEY, the name of the Senator from California (Mrs. FEINSTEIN) 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. 3085

At the request of Mr. MENENDEZ, the name of the Senator from Oregon (Mr. WYDEN) was added as a cosponsor of S. 3085, a bill to provide for the expansion of affordable refinancing of mortgages held by the Federal National Mortgage Association and the Federal Home Loan Mortgage Corporation.

S. 3204

At the request of Mr. JOHANNS, the names of the Senator from Wyoming (Mr. ENZI) and the Senator from Arizona (Mr. KYL) 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. 3340

At the request of Mrs. MURRAY, the name of the Senator from New Hampshire (Mrs. SHAHEEN) was added as a cosponsor of S. 3340, a bill to improve and enhance the programs and activities of the Department of Defense and the Department of Veterans Affairs regarding suicide prevention and resilience and behavioral health disorders for members of the Armed Forces and veterans, and for other purposes.

S. 3344

At the request of Mr. REED, the name of the Senator from Oregon (Mr. WYDEN) was added as a cosponsor of S. 3344, a bill to increase immunization rates.

S. 3354

At the request of Mr. CASEY, the name of the Senator from Connecticut (Mr. BLUMENTHAL) was added as a cosponsor of S. 3354, a bill to authorize the Transition Assistance Advisor program of the Department of Defense, and for other purposes.

S. 3383

At the request of Mr. VITTER, the name of the Senator from Alaska (Ms. MURKOWSKI) was added as a cosponsor of S. 3383, a bill to reject the final 5-year Outer Continental Shelf Oil and Gas Leasing Program for fiscal years 2012 through 2017 of the Administration and replace the plan with a 5-year plan that is more in line with the energy and economic needs of the United States.

S. 3394

At the request of Mr. JOHNSON of South Dakota, the name of the Senator from California (Mrs. FEINSTEIN) was added as a cosponsor of S. 3394, a bill to address fee disclosure requirements under the Electronic Fund Transfer Act, to amend the Federal Deposit Insurance Act with respect to information provided to the Bureau of Consumer Financial Protection, and for other purposes.

S. 3430

At the request of Mrs. SHAHEEN, the name of the Senator from Maryland (Mr. CARDIN) was added as a cosponsor of S. 3430, a bill to amend the Public Health Service Act to foster more effective implementation and coordination of clinical care for people with pre-diabetes and diabetes.

S. 3450

At the request of Mr. COATS, the name of the Senator from Missouri (Mr. BLUNT) was added as a cosponsor of 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.

S. 3451

At the request of Mr. BEGICH, the name of the Senator from Alaska (Ms. MURKOWSKI) was added as a cosponsor of S. 3451, a bill to exempt certain air taxi services from taxes on transportation by air.

S. 3453

At the request of Mr. HARKIN, the name of the Senator from Virginia (Mr. WEBB) was added as a cosponsor of S.

3453, a bill to provide for an increase in the Federal minimum wage.

S. CON. RES. 50

At the request of Mr. RUBIO, the names of the Senator from Utah (Mr. LEE) and the Senator from New Jersey (Mr. MENENDEZ) were added as cosponsors of S. Con. Res. 50, a concurrent resolution expressing the sense of Congress regarding actions to preserve and advance the multistakeholder governance model under which the Internet has thrived.

S. RES. 525

At the request of Mr. NELSON of Florida, the names of the Senator from Indiana (Mr. LUGAR) and the Senator from Massachusetts (Mr. KERRY) were added as cosponsors of S. Res. 525, a resolution honoring the life and legacy of Oswaldo Paya Sardinas.

AMENDMENT NO. 2575

At the request of Mr. LAUTENBERG, the name of the Senator from Michigan (Mr. LEVIN) was added as a cosponsor of amendment No. 2575 intended to be proposed to S. 3414, a bill to enhance the security and resiliency of the cyber and communications infrastructure of the United States.

SUBMITTED RESOLUTIONS

SENATE RESOLUTION 533—DESIGNATING OCTOBER 2012 AS ''NATIONAL WORK AND FAMILY MONTH''

Mr. MERKLEY (for himself, Mr. CRAPO, Mr. CASEY, Mr. BLUMENTHAL, Mrs. MURRAY, Mr. BROWN of Ohio, Mr. AKAKA, and Mr. KOHL) submitted the following resolution; which was considered and agreed to:

S. RES. 533

Whereas, according to a report by WorldatWork, a nonprofit professional association with expertise in attracting, motivating, and retaining employees, the quality of workers' jobs and the supportiveness of the workplace of the workers are key predictors of the job productivity, job satisfaction, and commitment to the employer of those workers, as well as of the ability of the employer to retain those workers;

Whereas ''work-life balance'' refers to specific organizational practices, policies, and programs that are guided by a philosophy of active support for the efforts of employees to achieve success within and outside the workplace, such as caring for dependents, health and wellness, paid and unpaid time off, financial support, community involvement, and workplace culture;

Whereas numerous studies show that employers that offer effective work-life balance programs are better able to recruit more talented employees, maintain a happier, healthier, and less stressed workforce, and retain experienced employees, which produces a more productive and stable workforce with less voluntary turnover;

Whereas job flexibility often allows parents to be more involved in the lives of their children, and research demonstrates that parental involvement is associated with higher achievement in language and mathematics, improved behavior, greater academic persistence, and lower dropout rates in children;

Whereas military families have special work-family needs that often require robust policies and programs that provide flexibility to employees in unique circumstances;

Whereas studies report that family rituals, such as sitting down to dinner together and sharing activities on weekends and holidays, positively influence the health and development of children and that children who eat dinner with their families every day consume nearly a full serving more of fruits and vegetables per day than those who never eat dinner with their families or do so only occasionally; and

Whereas the month of October is an appropriate month to designate as National Work and Family Month: Now, therefore, be it

Resolved, That the Senate—

(1) designates October 2012 as ''National Work and Family Month'';

(2) recognizes the importance of work schedules that allow employees to spend time with their families to job productivity and healthy families;

(3) urges public officials, employers, employees, and the general public to work together to achieve more balance between work and family; and

(4) calls upon the people of the United States to observe National Work and Family Month with appropriate ceremonies and activities.

AMENDMENTS SUBMITTED AND PROPOSED

SA 2621. 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.

SA 2622. Mr. CHAMBLISS submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2623. Mr. CHAMBLISS submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2624. Mr. CHAMBLISS submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2625. Mr. CHAMBLISS submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2626. Mr. CHAMBLISS submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2627. Mr. CHAMBLISS submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2628. Mr. CHAMBLISS submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2629. Mr. CHAMBLISS submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2630. Ms. SNOWE submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2631. Ms. SNOWE submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2632. Ms. SNOWE submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2633. Ms. SNOWE submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2634. Ms. SNOWE submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2635. Ms. SNOWE submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2636. Ms. SNOWE submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2637. Ms. SNOWE submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2638. Mr. RUBIO submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2639. 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 2640. Mr. LEAHY (for himself and 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.

SA 2641. Mr. CARPER (for himself and Mr. BLUNT) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2642. Mr. LEVIN submitted an amendment intended to be proposed by him to the bill S. 3406, to authorize the extension of nondiscriminatory treatment (normal trade relations treatment) to products of the Russian Federation and Moldova, to require reports on the compliance of the Russian Federation with its obligations as a member of the World Trade Organization, and to impose sanctions on persons responsible for gross violations of human rights, and for other purposes; which was ordered to lie on the table.

SA 2643. 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.

SA 2644. Mr. TOOMEY (for himself, Ms. SNOWE, Mr. DEMINT, Mr. BLUNT, Mr. RUBIO, and Mr. HELLER) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2645. Mr. BINGAMAN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2646. Mr. MENENDEZ (for himself and Mr. KERRY) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2647. Ms. SNOWE submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2648. Mr. LEVIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2649. Mr. LEVIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2650. Mr. UDALL of Colorado submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2651. Mr. UDALL of Colorado submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2652. Mr. UDALL of Colorado submitted an amendment intended to be proposed by

him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2653. Mr. GRAHAM submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2654. Mr. CRAPO (for himself and Mr. JOHANNS) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2655. 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 2656. 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 2657. 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 2658. 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 2659. 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 2660. 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 2661. 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 2662. 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 2663. 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 2664. 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.

TEXT OF AMENDMENTS

SA 2621. 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. ___. BORDER FENCE COMPLETION.

(a) MINIMUM REQUIREMENTS.—Section 102(b)(1) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1103 note) is amended—

(1) in subparagraph (A), by adding at the end the following: ''Fencing that does not effectively restrain pedestrian traffic (such as vehicle barriers and virtual fencing) may not be used to meet the 700-mile fence requirement under this subparagraph.'';

(2) in subparagraph (B)—

(A) in clause (i), by striking ''and'' at the end;

(B) in clause (ii), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(iii) not later than 1 year after the date of the enactment of the Cybersecurity Act of 2012, complete the construction of all the reinforced fencing and the installation of the related equipment described in subparagraph (A).''; and

(3) in subparagraph (C), by adding at the end the following:

''(iii) FUNDING NOT CONTINGENT ON CONSULTATION.—Amounts appropriated to carry out this paragraph may not be impounded or otherwise withheld for failure to fully comply with the consultation requirement under clause (i).''.

(b) REPORT.—Not later than 6 months after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to Congress a report that describes—

(1) the progress made in completing the reinforced fencing required under section 102(b)(1) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1103 note), as amended by subsection (a); and

(2) the plans for completing such fencing not later than 1 year after the date of the enactment of this Act.

SA 2622. Mr. CHAMBLISS 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 2623. Mr. CHAMBLISS 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, employeee, 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 2624. Mr. CHAMBLISS 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 VII.

SA 2625. Mr. CHAMBLISS 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 VII and insert the following:

TITLE VII—FACILITATING SHARING OF CYBER THREAT INFORMATION

SEC. 701. 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, employeee, 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. 702. 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. 703. 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 702, 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. 704. 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 702(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 702(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 702 for any use other than a use permitted under subsection 702(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. 705. 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 703 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 702 of this Act, including whether such information meets the definition of cyber threat information under section 701, 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 702 of this Act, including the appropriateness of any subsequent use under section 702(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 703 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. 706. 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. 707. 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 702 of title I of the Cybersecurity Act of 2012.''.

SEC. 708. 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.

SA 2626. Mr. CHAMBLISS 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 30, strike line 10, and all that follows through page 31, line 21, and insert the following:

(1) LIABILITY.—

(A) IN GENERAL.—No cause of action shall lie or be maintained in any court against a certified owner for any cyber-related incident that has impacted, or may impact, the information security of an information system of such owner, if such owner has been found to be in compliance with applicable cybersecurity practices through an assessment under subsection (b).

(B) ONGOING ASSESSMENT.—No cause of action shall lie or be maintained in any court against an owner or operator for any cyber-related incident that has impacted, or may impact, the information security of an information system of such owner or operator, if such owner or operator is, in good faith, in the process of obtaining, disputing, or satisfying the findings of an assessment under subsection (b).

(C) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this title shall be construed to subject any owner or operator for choosing not to engage in the voluntary activities authorized under this title.

(D) REMOVAL.—Any civil action arising from a cyber-related incident that has impacted, or may impact, the information security of an information system of an owner or operator engaged in the voluntary activities authorized under this title that is brought in a State court against any owner or operator shall be deemed to arise under the Constitution and laws of the United States and shall be removable under section 1441 of title 28, United States Code.

SA 2627. Mr. CHAMBLISS 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 23, strike line 18, and all that follows through page 25, line 8.

SA 2628. Mr. CHAMBLISS 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—EFFECTIVE DATE

SEC. 801. EFFECTIVE DATE.

(a) IN GENERAL.—This Act and the amendments made by this Act shall be effective during the 3-year period beginning on the date of the enactment of this Act.

(b) TRANSITION PROCEDURES.—Notwithstanding subsection (a), the limitations of liability in section 104(c)(1) and section 706 shall continue to apply to any actions described in such sections.

SA 2629. Mr. CHAMBLISS 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 9, strike line 7, and all that follows through page 25, line 24, and insert the following:

(b) MEMBERSHIP.—The Council shall be comprised of appropriate representatives appointed by the President from—

(1) the Department of Commerce;

(2) the Department of Defense;

(3) the Department of Justice;

(4) the intelligence community;

(5) sector-specific Federal agencies, as appropriate;

(6) Federal agencies with responsibility for regulating the security of critical cyber infrastructure, as appropriate; and

(7) the Department.

SEC. 102. VOLUNTARY CYBERSECURITY PRACTICES.

Not later than 180 days after the date of enactment of this Act, each sector coordinating council shall establish and maintain voluntary cybersecurity practices sufficient to effectively remediate or mitigate cyber risks identified by such sector coordinating council.

SA 2630. Ms. SNOWE 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:

At the end, add the following:

TITLE VIII—MISCELLANEOUS

SEC. 801. LIMITATIONS ON BILLS IMPLEMENTING TRADE AGREEMENTS.

(a) IN GENERAL.—Notwithstanding section 151 of the Trade Act of 1974 (19 U.S.C. 2191) or any other provision of law, any bill implementing a trade agreement between the United States and a country described in subsection (b) shall be subject to a point of order pursuant to subsection (c).

(b) COUNTRY DESCRIBED.—A country described in this subsection is a country the government of which is identified as perpetrating foreign economic collection or industrial espionage that threatens the economic security of the United States in a report to Congress of the Office of the National Counterintelligence Executive.

(c) POINT OF ORDER IN SENATE.—

(1) IN GENERAL.—The Senate shall cease consideration of a bill to implement a trade agreement if—

(A) a point of order is made by any Senator against the bill because the bill implements a trade agreement between the United States and a country described in subsection (b); and

(B) the point of order is sustained by the presiding officer.

(2) WAIVERS AND APPEALS.—

(A) WAIVERS.—Before the presiding officer rules on a point of order described in paragraph (1), any Senator may move to waive the point of order and the motion to waive shall not be subject to amendment. A point of order described in paragraph (1) is waived only by the affirmative vote of a majority of the Members of the Senate, duly chosen and sworn.

(B) APPEALS.—After the presiding officer rules on a point of order under this paragraph, any Senator may appeal the ruling of the presiding officer on the point of order as it applies to some or all of the provisions on which the presiding officer ruled. A ruling of the presiding officer on a point of order described in paragraph (1) is sustained unless a majority of the Members of the Senate, duly chosen and sworn, vote not to sustain the ruling.

(C) DEBATE.—Debate on a motion to waive under subparagraph (A) or on an appeal of the ruling of the presiding officer under subparagraph (B) shall be limited to 1 hour. The time shall be equally divided between, and controlled by, the majority leader and the minority leader of the Senate, or their designees.

SA 2631. Ms. SNOWE 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:

At the end of title IV, add the following:

SEC. 416. STUDY AND REPORT ON CYBERWORK BY SMALL BUSINESS CONCERNS.

(a) DEFINITIONS.—In this section—

(1) the term ''covered Federal agency'' means—

(A) the Department of Homeland Security;

(B) the Department of Defense; and

(C) each element of the intelligence community;

(2) the term ''intelligence community'' has the meaning given that term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)); and

(3) the term ''small business concern'' has the meaning given that term under section 3 of the Small Business Act (15 U.S.C. 632).

(b) STUDY.—The heads of the covered Federal agencies, in consultation with the Administrator of the Small Business Administration, shall jointly conduct a study of cyberwork performed by small business concerns for the covered Federal agencies.

(c) REPORT.—Not later than 180 days after the date of enactment of this Act, the heads of the covered Federal agencies shall jointly submit to the Committee on Small Business and Entrepreneurship, the Committee on Armed Services, the Committee on Homeland Security and Governmental Affairs, and the Select Committee on Intelligence of the Senate and the Committee on Small Business, the Committee on Armed Services, the Committee on Homeland Security, and the Committee on Intelligence of the House of Representatives a report on the results of the study under subsection (b) that contains—

(1) the number of small business concerns with top secret or sensitive compartmented information site clearances and an evaluation of whether small business concerns are carrying out a proportional amount of cyberwork for covered Federal agencies;

(2) a description of challenges faced by small business concerns in—

(A) securing cyberwork with covered Federal agencies;

(B) securing classified information technology work with covered Federal agencies;

(C) securing sponsorship by covered Federal agencies for site security clearances;

(D) obtaining security clearances for employees; and

(E) matters relating to the matters described in subparagraphs (A), (B), (C), and (D);

(3) recommendations for overcoming the challenges described in paragraph (2);

(4) an evaluation of the feasibility of and benefits to the Federal Government, the private sector, and small business concerns of establishing a program that would use small business concerns as incubators for developing cyberworkers who have top secret or sensitive compartmented information security clearances while the small business concerns perform other cyberwork for covered Federal agencies; and

(5) recommendations, if any, for legislation that would enable covered Federal agencies to better use the talents of small business concerns for cleared cyberwork.

SA 2632. Ms. SNOWE 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:

On page 108, line 6, insert '', including through the use of quantum entanglement for secured satellite and other point-to-point wireless communications'' before the semicolon.

SA 2633. Ms. SNOWE 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:

On page 150, strike line 24 and all that follows through page 151, line 8, and insert the following:

Congress reports—

(1) on available technical options, consistent with constitutional and statutory privacy rights, for enhancing the security of the information networks of entities that own or manage critical infrastructure through—

(A) technical improvements, including developing a secure domain; or

(B) increased notice of and consent to the use of technologies to scan for, detect, and defeat cyber security threats, such as technologies used in a secure domain; and

(2) providing an evaluation of the effort to implement the Domain Name System Security Extensions by owners and operators of critical infrastructure and Internet service providers, which shall—

(A) identify challenges hampering implementation; and

(B) provide proposals—

(i) to resolve any challenges identified under subparagraph (A); and

(ii) regarding how owners and operators of critical infrastructure and Internet service providers can streamline implementation of Domain Name System Security Extensions.

SA 2634. Ms. SNOWE 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:

At the end, add the following:

TITLE VIII—FCC TECHNICAL EXPERTISE CAPACITY

SECTION 801. SHORT TITLE.

This title may be cited as the ''FCC Technical Expertise Capacity Heightening Act'' or the ''FCC TECH Act''.

SEC. 802. APPOINTMENT OF TECHNICAL STAFF.

Section 4(f)(2) of the Communications Act of 1934 (47 U.S.C. 154(f)(2)) is amended by inserting after the first sentence the following new sentence: ''Each commissioner may also appoint an electrical engineer or computer scientist to provide the commissioner technical consultation when appropriate and to interface with the Office of Engineering and Technology, Commission Bureaus, and other technical staff of the Commission for additional technical input and resources, provided that such engineer or scientist holds an undergraduate or graduate degree from an institution of higher education in their respective field of expertise.''.

SEC. 803. TECHNICAL POLICY AND PERSONNEL STUDY.

(a) STUDY.—

(1) REQUIREMENTS OF STUDY.—The Chairman of the Federal Communications Commission (referred to in this section as the ''Commission'') shall enter into an arrangement with the National Academy of Sciences to complete a study of the technical policy decision-making and the technical personnel at the Commission.

(2) CONTENTS.—The study required under paragraph (1) shall—

(A) review the technical policy decision making of the Commission, including if the Commission has the adequate resources and processes in place to properly evaluate and account for the technical aspects and impact of the Commission's regulatory rulemaking;

(B) review—

(i) the timeliness of the rulemaking process utilized by the Commission; and

(ii) the impact of regulatory delay on telecommunications innovation;

(C) based upon the review undertaken pursuant to subparagraph (B), make recommendations for the Commission to streamline its rulemaking process;

(D) evaluate the current staffing levels and skill sets of technical personnel at the Commission to determine if such staffing levels and skill sets are aligned with the current and future needs of the Commission, as well as with current and future issues that come or may come under the jurisdiction of the

Commission and shall include a recommendation on the appropriate number or percentage of technical personnel that should constitute the Commission workforce;

(E) examine the current technical staff and engineering recruiting procedures at the Commission and make recommendations on how the Commission can improve its efforts to hire and retain engineers and other technical staff members;

(F) examine—

(i) the reliance of the Commission on external contractors in the development of policy and in evaluating the technical aspects of services, devices, and issues that arise under the jurisdiction of the Commission; and

(ii) the potential costs and benefits of the development of ''in-house'' resources to perform the duties that are currently being outsourced to external contractors; and

(G) compare the decision-making process of the Commission with the decision-making process used by similar regulatory authorities in other industrialized countries, including the European Union, Japan, Canada, Australia, and the United Kingdom.

(b) REPORT.—The Commission shall transmit a report describing the results of the study and recommendations required by subsection (a) to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Energy and Commerce of the House of Representatives.

(c) OFFSET OF ADMINISTRATIVE COSTS.—Section 4(a) of Public Law 109–34 (47 U.S.C. 703(a)) is amended by striking ''annual'' and inserting ''biennial''.

SA 2635. Ms. SNOWE 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:

At the appropriate place, insert the following:

SEC. ___. SMALL BUSINESS REGULATORY TRANSPARENCY.

Section 609(d) of title 5, United States Code, is amended—

(1) in paragraph (2), by striking ''and'' at the end;

(2) in paragraph (3), by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following:

''(4) the Department of Homeland Security.''.

SA 2636. Ms. SNOWE 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:

At the end of title I, add the following:

SEC. 111. SMALL BUSINESS MEMBERSHIP ON THE CRITICAL INFRASTRUCTURE PARTNERSHIP ADVISORY COUNCIL.

The Secretary shall ensure that the members of the Critical Infrastructure Partnership Advisory Council include—

(1) a representative of the Office of Advocacy of the Small Business Administration; and

(2) the owner of a small business concern or an advocate for small business concerns from the private sector.

SA 2637. Ms. SNOWE 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:

At the end of title IV, add the following:

SEC. 416. REPORT BY SMALL BUSINESS INFORMATION SECURITY TASK FORCE.

Not later than 1 year after the date of enactment of this Act, the Small Business Information Security Task Force, in consultation with the Chief Counsel for Advocacy of the Small Business Administration, shall submit to Congress a report that—

(1) analyzes the impact of this Act, and the amendments made by this Act, on small business concerns; and

(2) describes methods for mitigating any costs or unnecessary burdens imposed on small business concerns by regulations issued under this Act or the amendments made by this Act.

SA 2638. Mr. RUBIO 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. ___. PROHIBITION ON TREASURY REGULATIONS WITH RESPECT TO INFORMATION REPORTING ON CERTAIN INTEREST PAID TO NONRESIDENT ALIENS.

Except to the extent provided in Treasury Regulations as in effect on February 21, 2011, the Secretary of the Treasury shall not require (by regulation or otherwise) that an information return be made by a payor of interest in the case of interest—

(1) which is described in section 871(i)(2)(A) of the Internal Revenue Code of 1986; and

(2) which is paid—

(A) to a nonresident alien; and

(B) on a deposit maintained at an office within the United States.

SA 2639. 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. ___. REPEAL OF RENEWABLE FUEL STANDARD.

Section 211 of the Clean Air Act (42 U.S.C. 7545) is amended by striking subsection (o).

SA 2640. Mr. LEAHY (for himself and 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:

Beginning on page 109, strike line 4 and all that follows through page 110, line 20, and insert the following:

(d) CYBERSECURITY MODELING AND TEST BEDS.—

(1) REVIEW.—Not later than 1 year after the date of enactment of this Act, the Director shall conduct a review of cybersecurity test beds in existence on the date of enactment of this Act to inform the program established under paragraph (2).

(2) ESTABLISHMENT OF PROGRAM.—

(A) IN GENERAL.—The Director of the National Science Foundation, the Secretary, and the Secretary of Commerce shall establish a program for the appropriate Federal agencies to award grants to institutions of higher education or research and development non-profit institutions and to provide funds to the military service academies and senior military colleges (as defined in section 2111a of title 10, United States Code) to establish cybersecurity test beds capable of realistic modeling of real-time cyber attacks and defenses. The test beds shall work to enhance the security of public systems and focus on enhancing the security of critical private sector systems such as those in the finance, energy, and other sectors.

(B) REQUIREMENTS.—

(i) SIZE OF TEST BEDS.—The test beds established under the program established under subparagraph (A) shall be sufficiently large in order to model the scale and complexity of real world networks and environments.

(ii) USE OF EXISTING TEST BEDS.—The test bed program established under subparagraph (A) shall build upon and expand test beds and cyber attack simulation, experiment, and distributed gaming tools developed by the Under Secretary of Homeland Security for Science and Technology prior to the date of enactment of this Act.

(3) PURPOSES.—The purposes of the program established under paragraph (2) shall be to—

(A) support the rapid development of new cybersecurity defenses, techniques, and processes by improving understanding and assessing the latest technologies in a real-world environment; and

(B) to improve understanding among private sector partners of the risk, magnitude, and consequences of cyber attacks.

(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, senior military colleges (as defined in section 2111a of title 10, United States Code), and universities and institutions of higher education, and relevant nonprofit organizations; and

---

SA 2641. Mr. CARPER (for himself and Mr. BLUNT) 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—ACCOUNT DATA SECURITY

SEC. 801. SHORT TITLE.

This title may be cited as the ''Data Security Act of 2012''.

SEC. 802. DEFINITIONS.

For purposes of this title, the following definitions shall apply:

(1) AFFILIATE.—The term ''affiliate'' means any company that controls, is controlled by, or is under common control with another company.

(2) AGENCY.—The term ''agency'' has the same meaning as in section 551(1) of title 5, United States Code.

(3) BREACH OF DATA SECURITY.—

(A) IN GENERAL.—The term ''breach of data security'' means the unauthorized acquisition of sensitive account information or sensitive personal information.

(B) EXCEPTION FOR DATA THAT IS NOT IN USABLE FORM.—

(i) IN GENERAL.—The term ''breach of data security'' does not include the unauthorized acquisition of sensitive account information or sensitive personal information that is maintained or communicated in a manner that is not usable—

(I) to commit identity theft; or

(II) to make fraudulent transactions on financial accounts.

(ii) RULE OF CONSTRUCTION.—For purposes of this subparagraph, information that is maintained or communicated in a manner that is not usable includes any information that is maintained or communicated in an encrypted, redacted, altered, edited, or coded form.

(4) COMMISSION.—The term ''Commission'' means the Federal Trade Commission.

(5) CONSUMER.—The term ''consumer'' means an individual.

(6) CONSUMER REPORTING AGENCY THAT COMPILES AND MAINTAINS FILES ON CONSUMERS ON A NATIONWIDE BASIS.—The term ''consumer reporting agency that compiles and maintains files on consumers on a nationwide basis'' has the same meaning as in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

(7) COVERED ENTITY.—

(A) IN GENERAL.—The term ''covered entity'' means any—

(i) entity, the business of which is engaging in financial activities, as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k));

(ii) financial institution, including any institution described in section 313.3(k) of title 16, Code of Federal Regulations, as in effect on the date of enactment of this Act;

(iii) entity that maintains or otherwise possesses information that is subject to section 628 of the Fair Credit Reporting Act (15 U.S.C. 1681w); or

(iv) other individual, partnership, corporation, trust, estate, cooperative, association, or entity that maintains or communicates sensitive account information or sensitive personal information.

(B) EXCEPTION.—The term ''covered entity'' does not include any agency or any other unit of Federal, State, or local government or any subdivision of such unit.

(8) FINANCIAL INSTITUTION.—The term ''financial institution'' has the same meaning as in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809).

(9) SENSITIVE ACCOUNT INFORMATION.—The term ''sensitive account information'' means a financial account number relating to a consumer, including a credit card number or debit card number, in combination with any security code, access code, password, or other personal identification information required to access the financial account.

(10) SENSITIVE PERSONAL INFORMATION.—

(A) IN GENERAL.—The term ''sensitive personal information'' means the first and last name, address, or telephone number of a consumer, in combination with any of the following relating to such consumer:

(i) Social security account number.

(ii) Driver's license number or equivalent State identification number.

(iii) Taxpayer identification number.

(B) EXCEPTION.—The term ''sensitive personal information'' does not include publicly available information that is lawfully made available to the general public from—

(i) Federal, State, or local government records; or

(ii) widely distributed media.

(11) SUBSTANTIAL HARM OR INCONVENIENCE.—

(A) IN GENERAL.—The term ''substantial harm or inconvenience'' means—

(i) material financial loss to, or civil or criminal penalties imposed on, a consumer, due to the unauthorized use of sensitive account information or sensitive personal information relating to such consumer; or

(ii) the need for a consumer to expend significant time and effort to correct erroneous information relating to the consumer, including information maintained by a consumer reporting agency, financial institution, or government entity, in order to avoid material financial loss, increased costs, or civil or criminal penalties, due to the unauthorized use of sensitive account information or sensitive personal information relating to such consumer.

(B) EXCEPTION.—The term ''substantial harm or inconvenience'' does not include—

(i) changing a financial account number or closing a financial account; or

(ii) harm or inconvenience that does not result from identity theft or account fraud.

SEC. 803. PROTECTION OF INFORMATION AND SECURITY BREACH NOTIFICATION.

(a) SECURITY PROCEDURES REQUIRED.—

(1) IN GENERAL.—Each covered entity shall implement, maintain, and enforce reasonable policies and procedures to protect the confidentiality and security of sensitive account information and sensitive personal information which is maintained or is being communicated by or on behalf of a covered entity, from the unauthorized use of such information that is reasonably likely to result in substantial harm or inconvenience to the consumer to whom such information relates.

(2) LIMITATION.—Any policy or procedure implemented or maintained under paragraph (1) shall be appropriate to the—

(A) size and complexity of a covered entity;

(B) nature and scope of the activities of such entity; and

(C) sensitivity of the consumer information to be protected.

(b) INVESTIGATION REQUIRED.—

(1) IN GENERAL.—If a covered entity determines that a breach of data security has or may have occurred in relation to sensitive account information or sensitive personal information that is maintained or is being communicated by, or on behalf of, such covered entity, the covered entity shall conduct an investigation—

(A) to assess the nature and scope of the breach;

(B) to identify any sensitive account information or sensitive personal information that may have been involved in the breach; and

(C) to determine if such information is reasonably likely to be misused in a manner causing substantial harm or inconvenience to the consumers to whom the information relates.

(2) NEURAL NETWORKS AND INFORMATION SECURITY PROGRAMS.—In determining the likelihood of misuse of sensitive account information under paragraph (1)(C), a covered entity shall consider whether any neural network or security program has detected, or is likely to detect or prevent, fraudulent transactions resulting from the breach of security.

(c) NOTICE REQUIRED.—If a covered entity determines under subsection (b)(1)(C) that sensitive account information or sensitive personal information involved in a breach of data security is reasonably likely to be misused in a manner causing substantial harm or inconvenience to the consumers to whom the information relates, such covered entity, or a third party acting on behalf of such covered entity, shall—

(1) notify, in the following order—

(A) the appropriate agency or authority identified in section 805;

(B) an appropriate law enforcement agency;

(C) any entity that owns, or is obligated on, a financial account to which the sensitive account information relates, if the breach involves a breach of sensitive account information;

(D) each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, if the breach involves sensitive personal information relating to 5,000 or more consumers; and

(E) all consumers to whom the sensitive account information or sensitive personal information relates; and

(2) take reasonable measures to restore the security and confidentiality of the sensitive account information or sensitive personal information involved in the breach.

(d) PRESUMED COMPLIANCE BY CERTAIN ENTITIES.—

(1) IN GENERAL.—An entity shall be deemed to be in compliance with—

(A) in the case of a financial institution—

(i) subsection (a), and any regulations prescribed under such subsection, if such institution maintains policies and procedures to protect the confidentiality and security of sensitive account information and sensitive personal information that are consistent with the policies and procedures of such institution that are designed to comply with the requirements of section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)) and any regulations or guidance prescribed under that section that are applicable to such institution; and

(ii) subsections (b) and (c), and any regulations prescribed under such subsections, if such financial institution—

(I)(aa) maintains policies and procedures to investigate and provide notice to consumers of breaches of data security that are consistent with the policies and procedures of such institution that are designed to comply with the investigation and notice requirements established by regulations or guidance under section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)) that are applicable to such institution; or

(bb) is an affiliate of a bank holding company that maintains policies and procedures to investigate and provide notice to consumers of breaches of data security that are consistent with the policies and procedures of a bank that is an affiliate of such institution, and that bank's policies and procedures are designed to comply with the investigation and notice requirements established by any regulations or guidance under section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)) that are applicable to that bank; and

(II) provides for notice to the entities described under subparagraphs (B), (C), and (D) of subsection (c)(1), if notice is provided to consumers pursuant to the policies and procedures of such institution described in subclause (I); and

(B) subsections (a), (b), and (c), if the entity is a covered entity for purposes of the regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d-2 note), to the extent that such entity is in compliance with such regulations.

(2) DEFINITIONS.—For purposes of this subsection, the terms ''bank holding company'' and ''bank'' have the same meanings as in section 2 of the Bank Holding Company Act of 1956 (12 U.S.C. 1841).

SEC. 804. IMPLEMENTING REGULATIONS.

(a) IN GENERAL.—Notwithstanding any other provision of law, and except as provided under section 806, the agencies and authorities identified in section 805, with respect to the covered entities that are subject to the respective enforcement authority of such agencies and authorities, shall prescribe regulations to implement this title.

(b) COORDINATION.—Each agency and authority required to prescribe regulations under subsection (a) shall consult and coordinate with each other agency and authority identified in section 805 so that, to the extent possible, the regulations prescribed by each agency and authority are consistent and comparable.

(c) METHOD OF PROVIDING NOTICE TO CONSUMERS.—The regulations required under subsection (a) shall—

(1) prescribe the methods by which a covered entity shall notify a consumer of a breach of data security under section 803; and

(2) allow a covered entity to provide such notice by—

(A) written, telephonic, or e-mail notification; or

(B) substitute notification, if providing written, telephonic, or e-mail notification is not feasible due to—

(i) lack of sufficient contact information for the consumers that must be notified; or

(ii) excessive cost to the covered entity.

(d) CONTENT OF CONSUMER NOTICE.—The regulations required under subsection (a) shall—

(1) prescribe the content that shall be included in a notice of a breach of data security that is required to be provided to consumers under section 803; and

(2) require such notice to include—

(A) a description of the type of sensitive account information or sensitive personal information involved in the breach of data security;

(B) a general description of the actions taken by the covered entity to restore the security and confidentiality of the sensitive account information or sensitive personal information involved in the breach of data security; and

(C) the summary of rights of victims of identity theft prepared by the Commission under section 609(d) of the Fair Credit Reporting Act (15 U.S.C. 1681g), if the breach of data security involves sensitive personal information.

(e) TIMING OF NOTICE.—The regulations required under subsection (a) shall establish standards for when a covered entity shall provide any notice required under section 803.

(f) LAW ENFORCEMENT DELAY.—The regulations required under subsection (a) shall allow a covered entity to delay providing notice of a breach of data security to consumers under section 803 if a law enforcement agency requests such a delay in writing.

(g) SERVICE PROVIDERS.—The regulations required under subsection (a) shall—

(1) require any party that maintains or communicates sensitive account information or sensitive personal information on behalf of a covered entity to provide notice to that covered entity if such party determines that a breach of data security has, or may have, occurred with respect to such information; and

(2) ensure that there is only 1 notification responsibility with respect to a breach of data security.

(h) TIMING OF REGULATIONS.—The regulations required under subsection (a) shall—

(1) be issued in final form not later than 6 months after the date of enactment of this Act; and

(2) take effect not later than 6 months after the date on which they are issued in final form.

SEC. 805. ADMINISTRATIVE ENFORCEMENT.

(a) IN GENERAL.—Notwithstanding any other provision of law, section 803, and the regulations required under section 804, shall be enforced exclusively under—

(1) section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), in the case of—

(A) a national bank, a Federal branch or Federal agency of a foreign bank, or any subsidiary thereof (other than a broker, dealer, person providing insurance, investment company, or investment adviser), or a savings association, the deposits of which are insured by the Federal Deposit Insurance Corporation, or any subsidiary thereof (other than a broker, dealer, person providing insurance, investment company, or investment adviser), by the Office of the Comptroller of the Currency;

(B) a member bank of the Federal Reserve System (other than a national bank), a branch or agency of a foreign bank (other than a Federal branch, Federal agency, or insured State branch of a foreign bank), a commercial lending company owned or controlled by a foreign bank, an organization operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 601, 604), or a bank holding company and its nonbank subsidiary or affiliate (other than a broker, dealer, person providing insurance, investment company, or investment adviser), by the Board of Governors of the Federal Reserve System; and

(C) a bank, the deposits of which are insured by the Federal Deposit Insurance Corporation (other than a member of the Federal Reserve System), an insured State branch of a foreign bank, or any subsidiary thereof (other than a broker, dealer, person providing insurance, investment company, or investment adviser), by the Board of Directors of the Federal Deposit Insurance Corporation;

(2) the Federal Credit Union Act (12 U.S.C. 1751 et seq.), by the National Credit Union Administration Board with respect to any federally insured credit union;

(3) the Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.), by the Securities and Exchange Commission with respect to any broker or dealer;

(4) the Investment Company Act of 1940 (15 U.S.C. 80a–1 et seq.), by the Securities and Exchange Commission with respect to any investment company;

(5) the Investment Advisers Act of 1940 (15 U.S.C. 80b–1 et seq.), by the Securities and Exchange Commission with respect to any investment adviser registered with the Securities and Exchange Commission under that Act;

(6) the Commodity Exchange Act (7 U.S.C. 1 et seq.), by the Commodity Futures Trading Commission with respect to any futures commission merchant, commodity trading advisor, commodity pool operator, or introducing broker;

(7) the provisions of title XIII of the Housing and Community Development Act of 1992 (12 U.S.C. 4501 et seq.), by the Director of Federal Housing Enterprise Oversight (and any successor to such functional regulatory agency) with respect to the Federal National Mortgage Association, the Federal Home Loan Mortgage Corporation, and any other entity or enterprise (as defined in that title) subject to the jurisdiction of such functional regulatory agency under that title, including any affiliate of any such enterprise;

(8) State insurance law, in the case of any person engaged in providing insurance, by the applicable State insurance authority of the State in which the person is domiciled; and

(9) the Federal Trade Commission Act (15 U.S.C. 41 et seq.), by the Commission for any other covered entity that is not subject to the jurisdiction of any agency or authority described under paragraphs (1) through (8).

(b) EXTENSION OF FEDERAL TRADE COMMISSION ENFORCEMENT AUTHORITY.—The authority of the Commission to enforce compliance with section 803, and the regulations required under section 804, under subsection (a)(8) shall—

(1) notwithstanding the Federal Aviation Act of 1958 (49 U.S.C. App. 1301 et seq.), include the authority to enforce compliance by air carriers and foreign air carriers; and

(2) notwithstanding the Packers and Stockyards Act (7 U.S.C. 181 et seq.), include the authority to enforce compliance by persons, partnerships, and corporations subject to the provisions of that Act.

(c) NO PRIVATE RIGHT OF ACTION.—

(1) IN GENERAL.—This title, and the regulations prescribed under this title, may not be construed to provide a private right of action, including a class action with respect to any act or practice regulated under this title.

(2) CIVIL AND CRIMINAL ACTIONS.—No civil or criminal action relating to any act or practice governed under this title, or the regulations prescribed under this title, shall be commenced or maintained in any State court or under State law, including a pendent State claim to an action under Federal law.

SEC. 806. PROTECTION OF INFORMATION AT FEDERAL AGENCIES.

(a) DATA SECURITY STANDARDS.—Each agency shall implement appropriate standards relating to administrative, technical, and physical safeguards—

(1) to insure the security and confidentiality of the sensitive account information and sensitive personal information that is maintained or is being communicated by, or on behalf of, that agency;

(2) to protect against any anticipated threats or hazards to the security of such information; and

(3) to protect against misuse of such information, which could result in substantial harm or inconvenience to a consumer.

(b) SECURITY BREACH NOTIFICATION STANDARDS.—Each agency shall implement appropriate standards providing for notification of consumers when such agency determines that sensitive account information or sensitive personal information that is maintained or is being communicated by, or on behalf of, such agency—

(1) has been acquired without authorization; and

(2) is reasonably likely to be misused in a manner causing substantial harm or inconvenience to the consumers to whom the information relates.

SEC. 807. RELATION TO STATE LAW.

No requirement or prohibition may be imposed under the laws of any State with respect to the responsibilities of any person to—

(1) protect the security of information relating to consumers that is maintained or communicated by, or on behalf of, such person;

(2) safeguard information relating to consumers from potential misuse;

(3) investigate or provide notice of the unauthorized access to information relating to consumers, or the potential misuse of such information for fraudulent, illegal, or other purposes; or

(4) mitigate any loss or harm resulting from the unauthorized access or misuse of information relating to consumers.

SEC. 808. DELAYED EFFECTIVE DATE FOR CERTAIN PROVISIONS.

(a) COVERED ENTITIES.—Sections 803 and 807 shall take effect on the later of—

(1) 1 year after the date of enactment of this Act; or

(2) the effective date of the final regulations required under section 804.

(b) AGENCIES.—Section 806 shall take effect 1 year after the date of enactment of this Act.

SA 2642. Mr. LEVIN submitted an amendment intended to be proposed by him to the bill S. 3406, to authorize the extension of nondiscriminatory treatment (normal trade relations treatment) to products of the Russian Federation and Moldova, to require reports on the compliance of the Russian Federation with its obligations as a member of the World Trade Organization, and to impose sanctions on persons responsible for gross violations of human rights, and for other purposes; which was ordered to lie on the table; as follows:

On page 25, line 14, insert ''or any other foreign government'' before the semicolon.

SA 2643. 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:

On page 8, after line 22, insert the following:

SEC. 3. EFFECTIVE DATE.

(a) IN GENERAL.—Except as provided in subsection (b)(2), this Act and the amendments made by this Act shall not take effect until the date on which the Congressional Budget Office submits to Congress a report regarding the budgetary effects of this Act.

(b) CBO SCORE.—

(1) REPORT.—The Congressional Budget Office shall submit to Congress a report regarding the budgetary effects of this Act.

(2) EFFECTIVE DATE.—Paragraph (1) shall take effect on the date of enactment of this Act.

SA 2644. Mr. TOOMEY (for himself, Ms. SNOWE, Mr. DEMINT, Mr. BLUNT, Mr. RUBIO, and Mr. HELLER) 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—DATA SECURITY AND BREACH NOTIFICATION

SEC. 801. REQUIREMENTS FOR INFORMATION SECURITY.

Each covered entity shall take reasonable measures to protect and secure data in electronic form containing personal information.

SEC. 802. NOTIFICATION OF INFORMATION SECURITY BREACH.

(a) NOTIFICATION.—

(1) IN GENERAL.—A covered entity that owns or licenses data in electronic form containing personal information shall give notice of any breach of the security of the system following discovery by the covered entity of the breach of the security of the system to each individual who is a citizen or resident of the United States whose personal information was or that the covered entity reasonably believes to have been accessed and acquired by an unauthorized person and that the covered entity reasonably believes has caused or will cause, identity theft or other financial harm.

(2) LAW ENFORCEMENT.—A covered entity shall notify the Secret Service or the Federal Bureau of Investigation of the fact that a breach of security has occurred if the number of individuals whose personal information the covered entity reasonably believes to have been accessed and acquired by an unauthorized person exceeds 10,000.

(b) SPECIAL NOTIFICATION REQUIREMENTS.—

(1) THIRD-PARTY AGENTS.—

(A) IN GENERAL.—In the event of a breach of security of a system maintained by a third-party entity that has been contracted to maintain, store, or process data in electronic form containing personal information on behalf of a covered entity who owns or possesses such data, such third-party entity shall notify such covered entity of the breach of security.

(B) COVERED ENTITIES WHO RECEIVE NOTICE FROM THIRD PARTIES.—Upon receiving notification from a third party under subparagraph (A), a covered entity shall provide notification as required under subsection (a).

(C) EXCEPTION FOR SERVICE PROVIDERS.—A service provider shall not be considered a third-party agent for purposes of this paragraph.

(2) SERVICE PROVIDERS.—

(A) IN GENERAL.—If a service provider becomes aware of a breach of security involving data in electronic form containing personal information that is owned or possessed by a covered entity that connects to or uses a system or network provided by the service provider for the purpose of transmitting, routing, or providing intermediate or transient storage of such data, such service provider shall notify the covered entity who initiated such connection, transmission, routing, or storage if such covered entity can be reasonably identified.

(B) COVERED ENTITIES WHO RECEIVE NOTICE FROM SERVICE PROVIDERS.—Upon receiving notification from a service provider under subparagraph (A), a covered entity shall provide notification as required under subsection (a).

(c) TIMELINESS OF NOTIFICATION.—

(1) IN GENERAL.—Unless subject to a delay authorized under paragraph (2), a notification required under subsection (a) with respect to a security breach shall be made as expeditiously as practicable and without unreasonable delay, consistent with any measures necessary to determine the scope of the security breach and restore the reasonable integrity of the data system that was breached.

(2) DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT OR NATIONAL SECURITY PURPOSES.—

(A) LAW ENFORCEMENT.—If a Federal law enforcement agency determines that the notification required under subsection (a) would impede a civil or criminal investigation, such notification shall be delayed upon the written request of the law enforcement agency for any period which the law enforcement agency determines is reasonably necessary. A law enforcement agency may, by a subsequent written request, revoke such delay or extend the period set forth in the original request made under this subparagraph by a subsequent request if further delay is necessary.

(B) NATIONAL SECURITY.—If a Federal national security agency or homeland security agency determines that the notification required under this section would threaten national or homeland security, such notification may be delayed upon the written request of the national security agency or homeland security agency for any period which the national security agency or homeland security agency determines is reasonably necessary. A Federal national security agency or homeland security agency may revoke such delay or extend the period set forth in the original request made under this subparagraph by a subsequent written request if further delay is necessary.

(d) METHOD AND CONTENT OF NOTIFICATION.—

(1) DIRECT NOTIFICATION.—

(A) METHOD OF NOTIFICATION.—A covered entity required to provide notification to an individual under subsection (a) shall be in compliance with such requirement if the covered entity provides such notice by one of the following methods:

(i) Written notification, sent to the postal address of the individual in the records of the covered entity.

(ii) Telephone.

(iii) Email or other electronic means.

(B) CONTENT OF NOTIFICATION.—Regardless of the method by which notification is provided to an individual under subparagraph (A) with respect to a security breach, such notification, to the extent practicable, shall include—

(i) the date, estimated date, or estimated date range of the breach of security;

(ii) a description of the personal information that was accessed and acquired, or reasonably believed to have been accessed and acquired, by an unauthorized person as a part of the security breach; and

(iii) information that the individual can use to contact the covered entity to inquire about—

(I) the breach of security; or

(II) the information the covered entity maintained about that individual.

(2) SUBSTITUTE NOTIFICATION.—

(A) CIRCUMSTANCES GIVING RISE TO SUBSTITUTE NOTIFICATION.—A covered entity required to provide notification to an individual under subsection (a) may provide substitute notification in lieu of the direct notification required by paragraph (1) if such direct notification is not feasible due to—

(i) excessive cost to the covered entity required to provide such notification relative to the resources of such covered entity; or

(ii) lack of sufficient contact information for the individual required to be notified.

(B) FORM OF SUBSTITUTE NOTIFICATION.—Such substitute notification shall include at least one of the following:

(i) A conspicuous notice on the Internet Web site of the covered entity (if such covered entity maintains such a Web site).

(ii) Notification in print and to broadcast media, including major media in metropolitan and rural areas where the individuals whose personal information was acquired reside.

(e) TREATMENT OF PERSONS GOVERNED BY OTHER FEDERAL LAW.—Except as provided in section 4(b), a covered entity who is in compliance with any other Federal law that requires such covered entity to provide notification to individuals following a breach of security shall be deemed to be in compliance with this section.

SEC. 803. APPLICATION AND ENFORCEMENT.

(a) GENERAL APPLICATION.—The requirements of sections 801 and 802 apply to—

(1) those persons, partnerships, or corporations over which the Commission has authority pursuant to section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)); and

(2) notwithstanding section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)), common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.).

(b) APPLICATION TO CABLE OPERATORS, SATELLITE OPERATORS, AND TELECOMMUNICATIONS CARRIERS.—Sections 222, 338, and 631 of the Communications Act of 1934 (47 U.S.C. 222, 338, and 551), and any regulations promulgated thereunder, shall not apply with respect to the information security practices,

including practices relating to the notification of unauthorized access to data in electronic form, of any covered entity otherwise subject to those sections.

(c) ENFORCEMENT BY FEDERAL TRADE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of section 801 or 802 shall be treated as an unfair or deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.

(2) POWERS OF COMMISSION.—

(A) IN GENERAL.—Except as provided in subsection (a), the Commission shall enforce this title in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this title.

(B) PRIVILEGES AND IMMUNITIES.—Any person who violates section 801 or 802 shall be subject to the penalties and entitled to the privileges and immunities provided in such Act.

(3) MAXIMUM TOTAL LIABILITY.—Notwithstanding the number of actions which may be brought against a covered entity under this subsection, the maximum civil penalty for which any covered entity may be liable under this subsection for all actions shall not exceed—

(A) $500,000 for all violations of section 801 resulting from the same related act or omission; and

(B) $500,000 for all violations of section 802 resulting from a single breach of security.

(d) NO PRIVATE CAUSE OF ACTION.—Nothing in this title shall be construed to establish a private cause of action against a person for a violation of this title.

SEC. 804. DEFINITIONS.

In this title:

(1) BREACH OF SECURITY.—The term ''breach of security'' means unauthorized access and acquisition of data in electronic form containing personal information.

(2) COMMISSION.—The term ''Commission'' means the Federal Trade Commission.

(3) COVERED ENTITY.—

(A) IN GENERAL.—The term ''covered entity'' means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or utilizes personal information.

(B) EXEMPTIONS.—The term ''covered entity'' does not include the following:

(i) Financial institutions subject to title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.).

(ii) An entity covered by the regulations issued under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (Public Law 104–191) to the extent that such entity is subject to the requirements of such regulations with respect to protected health information.

(4) DATA IN ELECTRONIC FORM.—The term ''data in electronic form'' means any data stored electronically or digitally on any computer system or other database and includes recordable tapes and other mass storage devices.

(5) PERSONAL INFORMATION.—

(A) IN GENERAL.—The term ''personal information'' means an individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:

(i) Social Security number.

(ii) Driver's license number, passport number, military identification number, or other similar number issued on a government document used to verify identity.

(iii) Financial account number, or credit or debit card number, and any required security code, access code, or password that is necessary to permit access to an individual's financial account.

(B) EXCLUSIONS.—

(i) PUBLIC RECORD INFORMATION.—Personal information does not include information obtained about an individual which has been lawfully made publicly available by a Federal, State, or local government entity or widely distributed by media.

(ii) ENCRYPTED, REDACTED, OR SECURED DATA.—Personal information does not include information that is encrypted, redacted, or secured by any other method or technology that renders the data elements unusable.

(6) SERVICE PROVIDER.—The term ''service provider'' means an entity that provides electronic data transmission, routing, intermediate, and transient storage, or connections to its system or network, where such entity providing such services does not select or modify the content of the electronic data, is not the sender or the intended recipient of the data, and does not differentiate personal information from other information that such entity transmits, routes, stores, or for which such entity provides connections. Any such entity shall be treated as a service provider under this title only to the extent that it is engaged in the provision of such transmission, routing, intermediate and transient storage, or connections.

SEC. 805. EFFECT ON OTHER LAWS.

This title preempts any law, rule, regulation, requirement, standard, or other provision having the force and effect of law of any State, or political subdivision of a State, relating to the protection or security of data in electronic form containing personal information or the notification of a breach of security.

SEC. 806. EFFECTIVE DATE.

This title shall take effect on the date that is 1 year after the date of enactment of this Act.

SA 2645. Mr. BINGAMAN 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—GRID CYBER SECURITY

SEC. 801. SHORT TITLE.

This title may be cited as the ''Grid Cyber Security Act''.

SEC. 802. CRITICAL ELECTRIC INFRASTRUCTURE.

Part II of the Federal Power Act (16 U.S.C. 824 et seq.) is amended by adding at the end the following:

''SEC. 224. CRITICAL ELECTRIC INFRASTRUCTURE.

''(a) DEFINITIONS.—In this section:

''(1) CRITICAL ELECTRIC INFRASTRUCTURE.—The term 'critical electric infrastructure' means systems and assets, whether physical or virtual, used for the generation, transmission, or distribution of electric energy affecting interstate commerce that, as determined by the Commission or the Secretary (as appropriate), are so vital to the United States that the incapacity or destruction of the systems and assets would have a debilitating impact on national security, national economic security, or national public health or safety.

''(2) CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—The term 'critical electric infrastructure information' means critical infrastructure information relating to critical electric infrastructure.

''(3) CRITICAL INFRASTRUCTURE INFORMATION.—The term 'critical infrastructure information' has the meaning given the term in section 212 of the Critical Infrastructure Information Act of 2002 (6 U.S.C. 131).

''(4) CYBER SECURITY THREAT.—The term 'cyber security threat' means the imminent danger of an act that disrupts, attempts to disrupt, or poses a significant risk of disrupting the operation of programmable electronic devices or communications networks (including hardware, software, and data) essential to the reliable operation of critical electric infrastructure.

''(5) CYBER SECURITY VULNERABILITY.—The term 'cyber security vulnerability' means a weakness or flaw in the design or operation of any programmable electronic device or communication network that exposes critical electric infrastructure to a cyber security threat.

''(6) ELECTRIC RELIABILITY ORGANIZATION.—The term 'Electric Reliability Organization' has the meaning given the term in section 215(a).

''(7) SECRETARY.—The term 'Secretary' means the Secretary of Energy.

''(b) AUTHORITY OF COMMISSION.—

''(1) INITIAL DETERMINATION.—Not later than 120 days after the date of enactment of this section, the Commission shall determine whether reliability standards established pursuant to section 215 are adequate to protect critical electric infrastructure from cyber security vulnerabilities.

''(2) INITIAL ORDER.—Unless the Commission determines that the reliability standards established pursuant to section 215 are adequate to protect critical electric infrastructure from cyber security vulnerabilities within 120 days after the date of enactment of this section, the Commission shall order the Electric Reliability Organization to submit to the Commission, not later than 180 days after the date of issuance of the order, a proposed reliability standard or a modification to a reliability standard that will provide adequate protection of critical electric infrastructure from cyber security vulnerabilities.

''(3) SUBSEQUENT DETERMINATIONS AND ORDERS.—If at any time following the issuance of the initial order under paragraph (2) the Commission determines that the reliability standards established pursuant to section 215 are inadequate to protect critical electric infrastructure from a cyber security vulnerability, the Commission shall order the Electric Reliability Organization to submit to the Commission, not later than 180 days after the date of the determination, a proposed reliability standard or a modification to a reliability standard that will provide adequate protection of critical electric infrastructure from the cyber security vulnerability.

''(4) RELIABILITY STANDARDS.—Any proposed reliability standard or modification to a reliability standard submitted pursuant to paragraph (2) or (3) shall be developed and approved in accordance with section 215(d).

''(5) ADDITIONAL TIME.—The Commission may, by order, grant the Electric Reliability Organization reasonable additional time to submit a proposed reliability standard or a modification to a reliability standard under paragraph (2) or (3).

''(c) EMERGENCY AUTHORITY OF SECRETARY.—

''(1) IN GENERAL.—If the Secretary determines that immediate action is necessary to protect critical electric infrastructure from a cyber security threat, the Secretary may require, by order, with or without notice, persons subject to the jurisdiction of the Commission under this section to take such actions as the Secretary determines will best avert or mitigate the cyber security threat.

''(2) COORDINATION WITH CANADA AND MEXICO.—In exercising the authority granted under this subsection, the Secretary is encouraged to consult and coordinate with the appropriate officials in Canada and Mexico responsible for the protection of cyber security of the interconnected North American electricity grid.

''(3) CONSULTATION.—Before exercising the authority granted under this subsection, to the extent practicable, taking into account the nature of the threat and urgency of need for action, the Secretary shall consult with the entities described in subsection (e)(1) and with officials at other Federal agencies, as appropriate, regarding implementation of actions that will effectively address the identified cyber security threat.

''(4) COST RECOVERY.—The Commission shall establish a mechanism that permits public utilities to recover prudently incurred costs required to implement immediate actions ordered by the Secretary under this subsection.

''(d) DURATION OF EXPEDITED OR EMERGENCY RULES OR ORDERS.—Any order issued by the Secretary under subsection (c) shall remain effective for not more than 90 days unless, during the 90 day-period, the Secretary—

''(1) gives interested persons an opportunity to submit written data, views, or arguments; and

''(2) affirms, amends, or repeals the rule or order.

''(e) JURISDICTION.—

''(1) IN GENERAL.—Notwithstanding section 201, this section shall apply to any entity that owns, controls, or operates critical electric infrastructure.

''(2) COVERED ENTITIES.—

''(A) IN GENERAL.—An entity described in paragraph (1) shall be subject to the jurisdiction of the Commission for purposes of—

''(i) carrying out this section; and

''(ii) applying the enforcement authorities of this Act with respect to this section.

''(B) JURISDICTION.—This subsection shall not make an electric utility or any other entity subject to the jurisdiction of the Commission for any other purpose.

''(3) ALASKA AND HAWAII EXCLUDED.—Except as provided in subsection (f), nothing in this section shall apply in the State of Alaska or Hawaii.

''(f) DEFENSE FACILITIES.—Not later than 1 year after the date of enactment of this section, the Secretary of Defense shall prepare, in consultation with the Secretary, the States of Alaska and Hawaii, the Territory of Guam, and the electric utilities that serve national defense facilities in those States and Territory, a comprehensive plan that identifies the emergency measures or actions that will be taken to protect the reliability of the electric power supply of the national defense facilities located in those States and Territory in the event of an imminent cybersecurity threat.

''(g) PROTECTION OF CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—

''(1) IN GENERAL.—Section 214 of the Critical Infrastructure Information Act of 2002 (6 U.S.C. 133) shall apply to critical electric infrastructure information submitted to the Commission or the Secretary under this section, or developed by a Federal power marketing administration or the Tennessee Valley Authority under this section or section 215, to the same extent as that section applies to critical infrastructure information voluntarily submitted to the Department of Homeland Security under that Act (6 U.S.C. 131 et seq.).

''(2) RULES PROHIBITING DISCLOSURE.—Notwithstanding section 552 of title 5, United States Code, the Secretary and the Commission shall prescribe regulations prohibiting disclosure of information obtained or developed in ensuring cyber security under this section if the Secretary or Commission, as appropriate, decides disclosing the information would be detrimental to the security of critical electric infrastructure.

''(3) PROCEDURES FOR SHARING INFORMATION.—

''(A) IN GENERAL.—The Secretary and the Commission shall establish procedures on the release of critical infrastructure information to entities subject to this section, to the extent necessary to enable the entities to implement rules or orders of the Commission or the Secretary.

''(B) REQUIREMENTS.—The procedures shall—

''(i) limit the redissemination of information described in subparagraph (A) to ensure that the information is not used for an unauthorized purpose;

''(ii) ensure the security and confidentiality of the information;

''(iii) protect the constitutional and statutory rights of any individuals who are subjects of the information; and

''(iv) provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.

''(h) ACCESS TO CLASSIFIED INFORMATION.—

''(1) 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 section without the appropriate security clearances.

''(2) SECURITY CLEARANCES.—The appropriate Federal agencies or departments shall cooperate with the Secretary or the Commission, to the maximum extent practicable consistent with applicable procedures and requirements, in expeditiously providing appropriate security clearances to individuals that have a need-to-know (as defined in section 6.1 of that Executive Order) classified information to carry out this section.

''(i) NUCLEAR SAFETY.—No order issued by the Secretary or the Commission under this section, no reliability standard issued or modified by the Electric Reliability Organization pursuant to this section, and no temporary emergency order issued by the Electric Reliability Organization under section 215(d)(7) shall require or authorize a licensee of the Nuclear Regulatory Commission to operate a facility licensed by the Nuclear Regulatory Commission in a manner inconsistent with the terms of the license of the facility.''.

SEC. 803. LIMITED ADDITION OF ERO AUTHORITY FOR CRITICAL ELECTRIC INFRASTRUCTURE.

Section 215(a)(1) of the Federal Power Act (16 U.S.C. 824o(a)(1)) is amended—

(1) in the first sentence—

(A) by redesignating subparagraphs (A) and (B) as clauses (i) and (ii), respectively, and indenting appropriately;

(B) by striking ''(1) The term'' and inserting the following:

''(1) BULK-POWER SYSTEM.—

''(A) IN GENERAL.—The term'';

(C) in clause (i) (as so redesignated), by striking ''and'' after the semicolon at the end;

(D) in clause (ii) (as so redesignated), by striking the period at the end and inserting ''; and'';

(E) by adding at the end the following:

''(iii) for purposes of section 224, facilities used for the local distribution of electric energy that the Commission determines to be critical electric infrastructure pursuant to section 224.''; and

(2) in the second sentence, by striking ''The term'' and inserting the following:

''(B) EXCLUSION.—Except as provided in subparagraph (A), the term''.

SEC. 804. LIMITATION.

Section 215(i) of the Federal Power Act (16 U.S.C. 824o(i)) is amended by adding at the end the following:

''(6) LIMITATION.—The ERO shall have authority to develop and enforce compliance with reliability standards and temporary emergency orders with respect to a facility used in the local distribution of electric energy only to the extent the Commission determines the facility is so vital to the United States that the incapacity or destruction of the facility would have a debilitating impact on national security, national economic security, or national public health or safety.''.

SEC. 805. TEMPORARY EMERGENCY ORDERS FOR CYBER SECURITY VULNERABILITIES.

Section 215(d) of the Federal Power Act (16 U.S.C. 824o(d)) is amended by adding at the end the following:

''(7) TEMPORARY EMERGENCY ORDERS FOR CYBER SECURITY VULNERABILITIES.—Notwithstanding paragraphs (1) through (6), if the Commission determines that immediate action is necessary to protect critical electric infrastructure for a cyber security vulnerability, the Commission may, without prior notice or hearing, after consulting the ERO, require the ERO—

''(A) to develop and issue a temporary emergency order to address the cyber security vulnerability;

''(B) to make the temporary emergency order immediately effective; and

''(C) to keep the temporary emergency order in effect until—

''(i) the ERO develops, and the Commission approves, a final reliability standard under this section; or

''(ii) the Commission authorizes the ERO to withdraw the temporary emergency order.''.

SEC. 806. EMP STUDY.

(a) DOE REPORT.—Not later than 3 years after the date of enactment of this Act, the Secretary of Energy, in consultation with appropriate experts at the National Laboratories (as defined in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801)), shall prepare and publish a report that assesses the susceptibility of critical electric infrastructure to electromagnetic pulse events and geomagnetic disturbances.

(b) CONTENTS.—The report under subsection (a) shall—

(1) examine the risk of electromagnetic pulse events and geomagnetic disturbances, using both computer-based simulations and experimental testing;

(2) assess the full spectrum of possible events and disturbances and the likelihood that the events and disturbances would cause significant disruption to the transmission and distribution of electric power; and

(3) seek to quantify and reduce uncertainties associated with estimates for electromagnetic pulse events and geomagnetic disturbances.

(c) FERC ASSESSMENT.—Not later than 1 year after publication of the report under subsection (a), the Federal Energy Regulatory Commission, in coordination with the Secretary of Energy and in consultation with electric utilities and the ERO (as defined in section 215(a) of the Federal Power Act (16 U.S.C. 824o(a)), shall submit to Congress an assessment of whether and to what extent infrastructure affecting the transmission of electric power in interstate commerce should be hardened against electromagnetic events and geomagnetic disturbances, including an estimate of the costs and benefits of options to harden the infrastructure.

SEC. 807. BUDGETARY EFFECTS.

The budgetary effects of this Act, for the purpose of complying with the Statutory Pay-As-You-Go-Act of 2010, shall be determined by reference to the latest statement titled ''Budgetary Effects of PAYGO Legislation'' for this Act, submitted for printing in the Congressional Record by the Chairman of the Senate Budget Committee, provided that such statement has been submitted prior to the vote on passage.

SA 2646. Mr. MENENDEZ (for himself and Mr. KERRY) 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 III, add the following:

SEC. 305. CYBERSECURITY UNIVERSITY-INDUSTRY TASK FORCE.

(a) ESTABLISHMENT OF UNIVERSITY-INDUSTRY TASK FORCE.—Not later than 180 days after the date of enactment of this Act, the Director of the Office of Science and Technology Policy shall convene a task force to explore mechanisms for carrying out collaborative research, development, education, and training activities for cybersecurity through a consortium, or other appropriate entity, with participants from institutions of higher education and industry.

(b) FUNCTIONS.—The task force established under subsection (a) 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 the consortium;

(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;

(3) define the roles and responsibilities for the participants from institutions of higher education and industry in such entity;

(4) propose guidelines for assigning intellectual property rights and for the transfer of research and development results to the private sector; and

(5) make recommendations for how such entity could be funded from Federal, State, and nongovernmental 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, including minority-serving institutions and community colleges, and from industry with knowledge and expertise in cybersecurity.

(d) REPORT.—Not later than 12 months after the date of enactment of this Act, the Director of the Office of Science and Technology Policy shall transmit to the Congress a report describing the findings and recommendations of the task force established under subsection (a).

(e) TERMINATION.—The task force established under subsection (a) shall terminate upon transmittal of the report required under subsection (d).

(f) COMPENSATION AND EXPENSES.—Members of the task force established under subsection (a) shall serve without compensation.

SEC. 306. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY RESEARCH AND DEVELOPMENT.

(a) NIST CYBERSECURITY CHECKLISTS, CONFIGURATION PROFILES, AND DEPLOYMENT RECOMMENDATIONS.—Subsection (c) of section 8 of the Cyber Security Research and Development Act (15 U.S.C. 7406) is amended to read as follows:

''(c) SECURITY AUTOMATION AND CHECKLISTS FOR GOVERNMENT SYSTEMS.—

''(1) IN GENERAL.—The Director of the National Institute of Standards and Technology shall develop, and revise as necessary, security automation standards, associated reference materials (including protocols), and checklists providing settings and option selections that minimize the security risks associated with each information technology hardware or software system and security tool that is, or is likely to become, widely used within the Federal Government in order to enable standardized and interoperable technologies, architectures, and frameworks for continuous monitoring of information security within the Federal Government.

''(2) PRIORITIES FOR DEVELOPMENT, IDENTIFICATION, REVISION, AND ADAPTATION.—The Director of the National Institute of Standards and Technology shall establish priorities for the development of standards, reference materials, and checklists under this subsection on the basis of—

''(A) the security risks associated with the use of each system;

''(B) the number of agencies that use a particular system or security tool;

''(C) the usefulness of the standards, reference materials, or checklists to Federal agencies that are users or potential users of the system;

''(D) the effectiveness of the associated standard, reference material, or checklist in creating or enabling continuous monitoring of information security; or

''(E) such other factors as the Director of the National Institute of Standards and Technology determines to be appropriate.

''(3) EXCLUDED SYSTEMS.—The Director of the National Institute of Standards and Technology may exclude from the requirements of paragraph (1) any information technology hardware or software system or security tool for which such Director determines that the development of a standard, reference material, or checklist is inappropriate because of the infrequency of use of the system, the obsolescence of the system, or the inutility or impracticability of developing a standard, reference material, or checklist for the system.

''(4) DISSEMINATION OF CHECKLISTS, CONFIGURATION PROFILES, AND DEPLOYMENT RECOMMENDATIONS.—The Director of the National Institute of Standards and Technology shall ensure that Federal agencies are informed of the availability of any standard, reference material, checklist, or other item developed under this subsection.

''(5) AGENCY USE REQUIREMENTS.—The development of standards, reference materials, and checklists under paragraph (1) for an information technology hardware or software system or tool does not—

''(A) require any Federal agency to select the specific settings or options recommended by the standard, reference material, or checklist for the system;

''(B) establish conditions or prerequisites for Federal agency procurement or deployment of any such system;

''(C) imply an endorsement of any such system by the Director of the National Institute of Standards and Technology; or

''(D) preclude any Federal agency from procuring or deploying other information technology hardware or software systems for which no such standard, reference material, or checklist has been developed, or identified under paragraph (1).''.

(b) NIST CYBERSECURITY RESEARCH AND DEVELOPMENT.—Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended by redesignating subsection (e) as subsection (f), and by inserting after subsection (d) the following:

''(e) INTRAMURAL SECURITY RESEARCH.—As part of the research activities conducted in accordance with subsection (d)(3), the Institute shall—

''(1) conduct a research program to develop a unifying and standardized identity, privilege, and access control management framework for the execution of a wide variety of resource protection policies and that is amenable to implementation within a wide variety of existing and emerging computing environments;

''(2) carry out research associated with improving the security of information systems and networks;

''(3) carry out research associated with improving the testing, measurement, usability, and assurance of information systems and networks; and

''(4) carry out research associated with improving security of industrial control systems.''.

(c) NIST IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.—The Director 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.

(d) FEDERAL GOVERNMENT CLOUD COMPUTING STRATEGY.—

(1) IN GENERAL.—The Director, in collaboration with the Federal Chief Information Officers Council, and in consultation with other relevant Federal agencies and stakeholders from the private sector, shall continue to develop and encourage the implementation of a comprehensive strategy for the use and adoption of cloud computing services by the Federal Government.

(2) ACTIVITIES.—In carrying out the strategy developed under subsection (a), the Director shall give consideration to activities that—

(A) accelerate the development, in collaboration with the private sector, of standards that address interoperability and portability of cloud computing services;

(B) advance the development of conformance testing performed by the private sector in support of cloud computing standardization; and

(C) support, in consultation with the private sector, the development of appropriate security frameworks and reference materials, and the identification of best practices, for use by Federal agencies to address security and privacy requirements to enable the use and adoption of cloud computing services, including activities—

(i) to ensure the physical security of cloud computing data centers and the data stored in such centers;

(ii) to ensure secure access to the data stored in cloud computing data centers;

(iii) to develop security standards as required under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3); and

(iv) to support the development of the automation of continuous monitoring systems.

SA 2647. Ms. SNOWE 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:

At the appropriate place, insert the following:

SEC. ___. SPECTRUM EFFICIENCY AND SECURITY FUND.

(a) RETENTION OF UNUSED FUNDS.—Section 118(d)(4) of the National Telecommunications and Information Administration Organization Act (47 U.S.C. 928(d)(4)) is amended by striking ''8 years'' and inserting ''20 years''.

(b) USE OF FUND FOR PLANNING AND RESEARCH.—

(1) IN GENERAL.—Section 118(c) of the National Telecommunications and Information Administration Organization Act (47 U.S.C. 928(c)) is amended to read as follows:

''(c) USES OF FUNDS.—The amounts in the Fund are authorized to be used—

''(1) to pay relocation costs;

''(2) to fund planning and research with the goal of improving the efficiency of Federal use of spectrum and security of Federal wireless networks and systems; and

''(3) to cover the costs of eligible Federal entities to upgrade their equipment and facilities as long as such upgrades include spectrum sharing, reuse, and layering, and result in more efficient use of spectrum and more secure networks and systems by such entities.''.

(2) CONFORMING AMENDMENT.—Section 118(d)(2) of the National Telecommunications and Information Administration Organization Act (47 U.S.C. 928(d)(2)) is amended, in the matter preceding subparagraph (A), by inserting ''to pay relocation costs'' after ''subsection''.

(c) NATIONAL SCIENCE FOUNDATION.—Section 118(e) of the National Telecommunications and Information Administration Organization Act (47 U.S.C. 928(e)) is amended by adding at the end the following:

''(3) ELIGIBLE FEDERAL ENTITY; NATIONAL SCIENCE FOUNDATION.—In this section, the term 'eligible Federal entity' shall include the National Science Foundation. As an eligible Federal entity, the National Science Foundation may submit to the Director of OMB requests for funds under this section to support spectrum research and experimental facilities by the Foundation, provided that such requests have, in the determination of the Director of OMB, in consultation with the NTIA, clear benefits to existing and future Federal users of spectrum. The Director of OMB shall give priority to research that improves spectral efficiency or security of wireless network or systems.''.

(d) SPECTRUM EFFICIENCY AND SECURITY FUND.—

(1) IN GENERAL.—Section 118 of the National Telecommunications and Information Administration Organization Act (47 U.S.C. 928) is amended—

(A) in the section heading, by striking ''**SPECTRUM RELOCATION FUND**'' and inserting ''**SPECTRUM EFFICIENCY AND SECURITY FUND**''; and

(B) in subsection (a), by striking ''Spectrum Relocation Fund'' and inserting ''Spectrum Efficiency and Security Fund''.

(2) TECHNICAL AND CONFORMING AMENDMENTS.—

(A) COMMUNICATIONS ACT OF 1934.—Section 309(j)(8)(D) of the Communications Act of 1934 (47 U.S.C. 309(j)(8)(D)) is amended—

(i) in clause (i), by striking ''Spectrum Relocation Fund'' and inserting ''Spectrum Efficiency and Security Fund''; and

(ii) in clause (ii), in the first sentence, by striking ''Spectrum Relocation Fund'' and inserting ''Spectrum Efficiency and Security Fund''.

(B) NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION ORGANIZATION ACT.—Section 113 of the National Telecommunications and Information Administration Organization Act (47 U.S.C. 923) is amended—

(i) in subsection (g)(3), in the first sentence, by striking ''Spectrum Relocation Fund'' and inserting ''Spectrum Efficiency and Security Fund''; and

(ii) in subsection (h)(2)(G)(i), by striking ''Spectrum Relocation Fund'' and inserting ''Spectrum Efficiency and Security Fund''.

SA 2648. Mr. LEVIN 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—MISCELLANEOUS

SEC. 801. ACTIONS TO ADDRESS FOREIGN ECONOMIC OR INDUSTRIAL ESPIONAGE IN CYBERSPACE.

(a) REPORT REQUIRED.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and annually thereafter, the Director of National Intelligence shall submit to the appropriate congressional committees a report on foreign economic and industrial espionage in cyberspace during the 12-month period preceding the submission of the report that—

(A) identifies—

(i) foreign countries that engage in economic or industrial espionage in cyberspace with respect to trade secrets owned by United States persons;

(ii) foreign countries identified under clause (i) that the Director determines engage in the most egregious economic or industrial espionage in cyberspace with respect to trade secrets owned by United States persons (in this section referred to as ''priority foreign countries'');

(iii) technologies developed by United States persons that—

(I) are targeted for economic or industrial espionage in cyberspace; and

(II) to the extent practicable, have been appropriated through such espionage; and

(iv) articles manufactured or otherwise produced using technologies described in clause (iii);

(B) describes the economic or industrial espionage engaged in by the foreign countries identified under subparagraph (A); and

(C) describes—

(i) actions taken by the Director and other Federal agencies to decrease the prevalence of economic or industrial espionage in cyberspace; and

(ii) the progress made in decreasing the prevalence of economic or industrial espionage in cyberspace.

(2) DETERMINATION OF FOREIGN COUNTRIES ENGAGING IN ECONOMIC OR INDUSTRIAL ESPIONAGE IN CYBERSPACE.—For purposes of paragraph (1)(A), the Director shall identify a foreign country as a foreign country that engages in economic or industrial espionage in cyberspace with respect to trade secrets owned by United States persons if the government of the foreign country—

(A) engages in economic or industrial espionage in cyberspace with respect to trade secrets owned by United States persons; or

(B) facilitates, supports, fails to prosecute, or otherwise tolerates such espionage by—

(i) individuals who are citizens or residents of the foreign country; or

(ii) entities that are organized under the laws of the foreign country or are otherwise subject to the jurisdiction of the government of the foreign country.

(3) FORM OF REPORT.—Each report required by paragraph (1) shall be submitted in unclassified form but may contain a classified annex.

(b) REFERRAL TO UNITED STATES INTERNATIONAL TRADE COMMISSION.—The Director of National Intelligence shall refer the report required by subsection (a) to the United States International Trade Commission for appropriate action under section 337 of the Tariff Act of 1930 (19 U.S.C. 1337).

(c) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Armed Services, the Committee on Homeland Security and Governmental Affairs, the Committee on Finance, the Committee on Foreign Relations, and the Select Committee on Intelligence of the Senate; and

(B) the Committee on Armed Services, the Committee on Homeland Security, the Committee on Foreign Affairs, the Committee on Ways and Means, and the Permanent Select Committee on Intelligence of the House of Representatives.

(2) CYBERSPACE.—The term ''cyberspace''—

(A) means the interdependent network of information technology infrastructures; and

(B) includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

(3) ECONOMIC OR INDUSTRIAL ESPIONAGE.—The term ''economic or industrial espionage'' means—

(A) stealing a trade secret or appropriating, taking, carrying away, or concealing, or by fraud, artifice, or deception obtaining, a trade secret without the authorization of the owner of the trade secret;

(B) copying, duplicating, downloading, uploading, destroying, transmitting, delivering, sending, communicating, or conveying a trade secret without the authorization of the owner of the trade secret; or

(C) knowingly receiving, buying, or possessing a trade secret that has been stolen or appropriated, obtained, or converted without the authorization of the owner of the trade secret.

(4) OWN.—The term ''own'', with respect to a trade secret, means to hold rightful legal or equitable title to, or license in, the trade secret.

(5) PERSON.—The term ''person'' means an individual or entity.

(6) TECHNOLOGY.—The term ''technology'' has the meaning given that term in section 16 of the Export Administration Act of 1979 (50 U.S.C. App. 2415) (as in effect pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.)).

(7) TRADE SECRET.—The term ''trade secret'' has the meaning given that term in section 1839 of title 18, United States Code.

(8) UNITED STATES PERSON.—The term ''United States person'' means—

(A) an individual who is a citizen of the United States or an alien lawfully admitted for permanent residence to the United States; or

(B) an entity organized under the laws of the United States or any jurisdiction within the United States.

SA 2649. Mr. LEVIN 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. REPORTS TO DEPARTMENT OF DEFENSE ON PENETRATIONS OF NETWORKS AND INFORMATION SYSTEMS OF CERTAIN CONTRACTORS.

(a) PROCESS FOR REPORTING PENETRATIONS.—The Under Secretary of Defense for

Intelligence shall, in coordination with the officials specified in subsection (c), establish a process by which cleared defense contractors shall report to elements of the Department of Defense designated by the Under Secretary for purposes of the process when a network or information system of such contractors designated pursuant to subsection (b) is successfully penetrated.

(b) DESIGNATION OF NETWORKS AND INFORMATION SYSTEMS.—The Under Secretary of Defense for Intelligence shall, in coordination with the officials specified in subsection (c), establish criteria for designating the cleared defense contractors' networks or information systems that contain or process information created by or for the Department of Defense to be subject to the reporting process established pursuant to subsection (a).

(c) OFFICIALS.—The officials specified in this subsection are the following:

(1) The Under Secretary of Defense for Policy.

(2) The Under Secretary of Defense for Acquisition, Technology, and Logistics.

(3) The Chief Information Officer of the Department of Defense.

(4) The Commander of the United States Cyber Command.

(d) PROCESS REQUIREMENTS.—

(1) RAPID REPORTING.—The process required by subsection (a) shall provide for rapid reporting by contractors of successful penetrations of designated network or information systems.

(2) REPORT ELEMENTS.—The report by a contractor on a successful penetration of a designated network or information system under the process shall include the following:

(A) A description of the technique or method used in the penetration.

(B) A sample of the malicious software, if discovered and isolated by the contractor.

(3) ACCESS.—The process shall include mechanisms by which Department of Defense personnel may, upon request, obtain access to equipment or information of a contractor necessary to conduct a forensic analysis to determine whether information created by or for the Department in connection with any Department program was successfully exfiltrated from a network or information system of the contractor and, if so, what information was exfiltrated.

(e) CLEARED DEFENSE CONTRACTOR DEFINED.—In this section, the term ''cleared defense contractor'' means a private entity granted clearance by the Defense Security Service to receive and store classified information for the purpose of bidding for a contract or conducting activities under a contract with the Department of Defense.

SA 2650. Mr. UDALL of Colorado 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 IV, add the following:

SEC. 416. CYBER TRAINING AND RESEARCH AT THE UNITED STATES AIR FORCE ACADEMY, COLORADO.

(a) FINDINGS.—Congress makes the following findings:

(1) The training of cyber security leaders is a critical function of the United States Air Force Academy.

(2) The Center for Cyberspace Research at the United States Air Force Academy has been instrumental in educating and developing highly skilled cyber innovators for the Department of Defense.

(3) The Center for Cyberspace Research benefits greatly from interagency funding, information-sharing, and other collaboration, and it is in the national interest that such funding, information-sharing and collaboration continue.

(4) The Cyber Training Range operated by the Computer Science Department at the United States Air Force Academy provides realistic cyber training for cadets that will benefit the entire Air Force.

(5) The establishment of a civilian director for the Cyberspace Research Center and the Cyber Training Range as permanent faculty positions at the United States Air Force Academy will help assure that the Center and Range are both maintained and staffed with highly-experienced cyber experts.

(b) SENSE OF CONGRESS.—It is the sense of Congress that the partner organizations for the Center for Cyberspace Research and the Cyber Training Range, including the Air Force Office of Scientific Research (AFOSR), the Defense Advanced Projects Research Agency (DARPA), the Defense Information Assurance Program (DIAP) of the Department of Defense, the National Security Agency, and the National Reconnaissance Office, maintain their funding, information-sharing, and other collaborative commitments to the Center for Cyberspace Research and the Cyber Training Range.

(c) CIVILIAN DIRECTOR FOR CENTER FOR CYBERSPACE RESEARCH.—

(1) IN GENERAL.—The head of the Center for Cyberspace Research at the United States Air Force Academy, Colorado, shall be the Director of the Center for Cyberspace Research, who shall be a civilian employee of the Air Force.

(2) PERMANENT BILLET IN EXCEPTED SERVICE.—The position of Director of the Center for Cyberspace Research shall be a permanent civilian billet in the excepted service (as that term is defined in section 2103(a) of title 5, United States Code).

(3) PAY GRADE.—The level of pay of the person serving in the position of Director of the Center for Cyberspace Research shall be a level of pay not below that payable for paygrade GS–14 of the General Schedule.

(d) CIVILIAN DIRECTOR FOR CYBER TRAINING RANGE.—

(1) IN GENERAL.—The head of the Cyber Training Range in the Computer Science Department of the United States Air Force Academy, Colorado, shall be the Director of the Cyber Training Range, who shall be a civilian employee of Air Force.

(2) PERMANENT BILLET IN EXCEPTED SERVICE.—The position of Director of the Cyber Training Range shall be a permanent civilian billet in the excepted service (as so defined).

(3) PAY GRADE.—The level of pay of the person serving in the position of Director of the Cyber Training Range shall be a level of pay not below that payable for paygrade GS–12 of the General Schedule.

(e) AMOUNTS AVAILABLE FOR PAY.—Amounts for the pay and allowances of the directors covered by subsections (c) and (d) shall be derived from amounts available to the Air Force for the pay and allowances of civilian employees of the Air Force.

SA 2651. Mr. UDALL of Colorado 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 IV, add the following:

SEC. 416. REPORT ON DOMESTIC PRODUCTION, SECURITY, AND AVAILABILITY OF EXTRA HIGH VOLTAGE TRANSFORMERS.

(a) FINDING.—Based on reports provided by the Department of Defense and the Department of Homeland Security, Congress finds that the lack of a secured stockpile of domestically-produced Extra High Voltage (EHV) transformers, and the current manufacturing backlog for Extra High Voltage transformers in the United States, are likely to contribute to extended blackouts and power shortages in the event of a physical or network-based attack on the electric power infrastructure of the United States.

(b) REPORT.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary shall, in collaboration with the Secretary of Defense, submit to the appropriate committees of Congress a report on the domestic production, security, and availability of Extra High Voltage transformers.

(2) ELEMENTS.—The report required by paragraph (1) shall include the following:

(A) An assessment whether the number of Extra High Voltage transformers currently held in reserve by utilities and public and private manufacturers in the United States is sufficient, and is secured in a manner adequate, to maintain national security operations in the event of loss or damage to multiple Extra High Voltage transformers in the United States, Canada, or Mexico.

(B) An identification and assessment of the risks associated with having no spare Extra High Voltage transformers stockpiled and securely stored for national security purposes.

(C) An estimate of the time that national security operations would be negatively impacted if two or more Extra High Voltage transformers in the United States were destroyed by cyber attack, physical attack, or a natural disaster.

(D) An estimate of the feasability and cost of establishing a stockpile of not fewer than 30, and as many 60, Extra High Voltage transformers at disbursed Department of Defense installations or other national security locations in the continental United States.

(E) Recommendation as to the best locations to store Extra High Voltage transformers stockpiled as described in subparagraph (D) in order to ensure security and the rapid distribution of such transformers in emergency circumstances.

(3) FORM.—The report required by paragraph (1) shall be submitted in unclassified form, and shall include a classified annex containing a detailed description of the relationship between national security functions and locations of Extra High Voltage Transformers.

(4) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this subsection, the term ''appropriate committees of Congress'' means—

(A) the Committee on Armed Services, the Committee on Homeland Security and Governmental Affairs, and the Committee on Appropriations of the Senate; and

(B) the Committee on Armed Services, the Committee on Oversight and Reform, and the Committee on Appropriations of the House of Representatives.

SA 2652. Mr. UDALL of Colorado 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 132, strike lines 16 through 21 and insert the following:

(2) CONTENTS.—The strategy developed under paragraph (1) shall include—

(A) a 5-year plan on recruitment of personnel for the Federal workforce that includes—

(i) a description of Federal programs for identifying, recruiting, training, and retaining individuals with outstanding computer skills for service in the Federal Government; and

(ii) a description of any bonuses or any non-traditional or non-standard recruiting practices that are employed by the Federal Government to locate and recruit individuals for career fields related to cybersecurity; and

(B) a 10-year projection of Federal workforce needs that includes an identification of any staffing or specialty shortfalls in career fields related to cybersecurity.

SA 2653. Mr. GRAHAM 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—IRANIAN NUCLEAR PROGRAM

SEC. 801. IRANIAN NUCLEAR PROGRAM.

(a) FINDINGS.—Congress makes the following findings:

(1) Since at least the late 1980s, the Government of the Islamic Republic of Iran has engaged in a sustained and well-documented pattern of illicit and deceptive activities to acquire nuclear capability.

(2) The United Nations Security Council has adopted multiple resolutions since 2006 demanding the full and sustained suspension of all uranium enrichment-related and reprocessing activities by the Government of the Islamic Republic of Iran and its full cooperation with the International Atomic Energy Agency (IAEA) on all outstanding issues related to its nuclear activities, particularly those concerning the possible military dimensions of its nuclear program.

(3) On November 8, 2011, the IAEA issued an extensive report that—

(A) documents ''serious concerns regarding possible military dimensions to Iran's nuclear programme'';

(B) states that ''Iran has carried out activities relevant to the development of a nuclear device''; and

(C) states that the efforts described in paragraphs (1) and (2) may be ongoing.

(4) As of November 2008, Iran had produced, according to the IAEA—

(A) approximately 630 kilograms of uranium hexaflouride enriched up to 3.5 percent uranium-235; and

(B) no uranium hexaflouride enriched up to 20 percent uranium-235.

(5) As of November 2011, Iran had produced, according to the IAEA—

(A) nearly 5,000 kilograms of uranium hexaflouride enriched up to 3.5 percent uranium-235; and

(B) 79.7 kilograms of uranium hexaflouride enriched up to 20 percent uranium-235.

(6) On January 9, 2012, IAEA inspectors confirmed that the Government of the Islamic Republic of Iran had begun enrichment activities at the Fordow site, including possibly enrichment of uranium hexaflouride up to 20 percent uranium-235.

(7) Section 2(2) of the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (Public Law 111–195) states, ''The United States and other responsible countries have a vital interest in working together to prevent the Government of Iran from acquiring a nuclear weapons capability.''.

(8) If the Government of the Islamic Republic of Iran were successful in acquiring a nuclear weapon capability, it would likely spur other countries in the region to consider developing their own nuclear weapons capabilities.

(9) On December 6, 2011, Prince Turki al-Faisal of Saudi Arabia stated that if international efforts to prevent Iran from obtaining nuclear weapons fail, ''we must, as a duty to our country and people, look into all options we are given, including obtaining these weapons ourselves''.

(10) Top leaders of the Government of the Islamic Republic of Iran have repeatedly threatened the existence of the State of Israel, pledging to ''wipe Israel off the map''.

(11) The Department of State has designated Iran as a state sponsor of terrorism since 1984 and characterized Iran as the ''most active state sponsor of terrorism''.

(12) The Government of the Islamic Republic of Iran has provided weapons, training, funding, and direction to terrorist groups, including Hamas, Hezbollah, and Shiite militias in Iraq that are responsible for the murders of hundreds of United States forces and innocent civilians.

(13) On July 28, 2011, the Department of the Treasury charged that the Government of Iran had forged a ''secret deal'' with al Qaeda to facilitate the movement of al Qaeda fighters and funding through Iranian territory.

(14) In October 2011, senior leaders of Iran's Islamic Revolutionary Guard Corps (IRGC) Quds Force were implicated in a terrorist plot to assassinate Saudi Arabia's Ambassador to the United States on United States soil.

(15) On December 26, 2011, the United Nations General Assembly passed a resolution denouncing the serious human rights abuses occurring in the Islamic Republic of Iran, including torture, cruel and degrading treatment in detention, the targeting of human rights defenders, violence against women, and ''the systematic and serious restrictions on freedom of peaceful assembly'' as well as severe restrictions on the rights to ''freedom of thought, conscience, religion or belief''.

(16) President Barack Obama, through the P5+1 process, has made repeated efforts to engage the Government of the Islamic Republic of Iran in dialogue about Iran's nuclear program and its international commitments under the Treaty on the Non-Proliferation of Nuclear Weapons, done at Washington, London, and Moscow July 1, 1968, and entered into force March 5, 1970 (commonly known as the ''Nuclear Non-Proliferation Treaty'').

(17) Representatives of the P5+1 countries (the United States, France, Germany, the People's Republic of China, the Russian Federation, and the United Kingdom) and representatives of the Islamic Republic of Iran held negotiations on Iran's nuclear program in Istanbul, Turkey on April 14, 2012, and these discussions are set to resume in Baghdad, Iraq on May 23, 2012.

(18) On March 31, 2010, President Obama stated that the ''consequences of a nuclear-armed Iran are unacceptable''.

(19) In his State of the Union Address on January 24, 2012, President Obama stated, ''Let there be no doubt: America is determined to prevent Iran from getting a nuclear weapon, and I will take no options off the table to achieve that goal.''.

(20) On March 4, 2012, President Obama stated ''Iran's leaders should understand that I do not have a policy of containment; I have a policy to prevent Iran from obtaining a nuclear weapon''.

(21) Secretary of Defense Leon Panetta stated, in December 2011, that it was unacceptable for Iran to acquire nuclear weapons, reaffirmed that all options were on the table to thwart Iran's nuclear weapons efforts, and vowed that if the United States gets ''intelligence that they are proceeding with developing a nuclear weapon then we will take whatever steps necessary to stop it''.

(22) The Department of Defense's January 2012 Strategic Guidance stated that United States defense efforts in the Middle East would be aimed ''to prevent Iran's development of a nuclear weapons capability and counter its destabilizing policies''.

(23) On April 2, 2010, President Obama stated, ''All the evidence indicates that the Iranians are trying to develop the capacity to develop nuclear weapons. They might decide that, once they have that capacity that they'd hold off right at the edge in order not to incur more sanctions. But, if they've got nuclear weapons-building capacity and they are flouting international resolutions, that creates huge destabilizing effects in the region and will trigger an arms race in the Middle East that is bad for U.S. national security but is also bad for the entire world.''.

(b) SENSE OF CONGRESS.—Congress—

(1) reaffirms that the United States Government and the governments of other responsible countries have a vital interest in working together to prevent the Government of Iran from acquiring a nuclear weapons capability;

(2) warns that time is limited to prevent the Government of the Islamic Republic of Iran from acquiring a nuclear weapons capability;

(3) urges continued and increasing economic and diplomatic pressure on the Islamic Republic of Iran until the Government of the Islamic Republic of Iran agrees to and implements—

(A) the full and sustained suspension of all uranium enrichment-related and reprocessing activities and compliance with United Nations Security Council resolutions;

(B) complete cooperation with the IAEA on all outstanding questions related to the nuclear activities of the Government of the Islamic Republic of Iran, including the implementation of the additional protocol to Iran's Safeguards Agreement with the IAEA; and

(C) a permanent agreement that verifiably assures that Iran's nuclear program is entirely peaceful;

(4) expresses the desire that the P5+1 process successfully and swiftly leads to the objectives identified in paragraph (3);

(5) warns that, as President Obama has said, the window for diplomacy is closing;

(6) expresses support for the universal rights and democratic aspirations of the people of Iran;

(7) strongly supports United States policy to prevent the Government of the Islamic Republic of Iran from acquiring a nuclear weapons capability;

(8) rejects any United States policy that would rely on efforts to contain a nuclear weapons-capable Iran; and

(9) joins the President in ruling out any policy that would rely on containment as an option in response to the Iranian nuclear threat.

(c) RULE OF CONSTRUCTION.—Nothing in this section may be construed as an authorization for the use of force or a declaration of war.

SA 2654. Mr. CRAPO (for himself and Mr. JOHANNS) 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:

SEC. ___. BUSINESS RISK MITIGATION AND PRICE STABILIZATION.

(a) MARGIN REQUIREMENTS.—

(1) COMMODITY EXCHANGE ACT AMENDMENT.—Section 4s(e) of the Commodity Exchange Act (7 U.S.C. 6s(e)), as added by section 731 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, is amended by adding at the end the following new paragraph:

''(4) APPLICABILITY WITH RESPECT TO COUNTERPARTIES.—The requirements of paragraphs (2)(A)(ii) and (2)(B)(ii) shall not apply to a swap in which a counterparty qualifies for an exception under section 2(h)(7)(A) or satisfies the criteria in section 2(h)(7)(D).''.

(2) SECURITIES EXCHANGE ACT AMENDMENT.—Section 15F(e) of the Securities Exchange Act of 1934 (15 U.S.C. 78o–10(e)), as added by section 764(a) of the Dodd-Frank Wall Street Reform and Consumer Protection Act, is amended by adding at the end the following new paragraph:

''(4) APPLICABILITY WITH RESPECT TO COUNTERPARTIES.—The requirements of paragraphs (2)(A)(ii) and (2)(B)(ii) shall not apply to a security-based swap in which a counterparty qualifies for an exception under section 3C(g)(1) or satisfies the criteria in section 3C(g)(4).''.

(b) IMPLEMENTATION.—The amendments made by this section to the Commodity Exchange Act shall be implemented—

(1) without regard to—

(A) chapter 35 of title 44, United States Code; and

(B) the notice and comment provisions of section 553 of title 5, United States Code;

(2) through the promulgation of an interim final rule, pursuant to which public comment will be sought before a final rule is issued; and

(3) such that paragraph (1) shall apply solely to changes to rules and regulations, or proposed rules and regulations, that are limited to and directly a consequence of such amendments.

SA 2655. 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 18 and all that follows through page 25, line 8.

SA 2656. 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 145, strike lines 5 through 11 and insert the following:

''(f) ANNUAL REPORT.—Not later than 1 year after

SA 2657. 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 124, strike line 7 and all that follows through page 128, line 14.

SA 2658. 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 121, strike lines 13 through 24.

SA 2659. 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 142, strike line 3 and all that follows through page 145, line 4.

SA 2660. 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 154, strike line 9 and all that follows through page 156, line 13.

SA 2661. 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 122, strike line 1 and all that follows through page 124, line 6.

SA 2662. 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 3 years after the date of enactment of this Act.

SA 2663. 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 5 years after the date of enactment of this Act.

SA 2664. 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 122, strike lines 18 through 25, and insert the following:

vulnerabilities; and

(2) in accordance with subsection (d), a program for carrying out collaborative education and

---

PRIVILEGES OF THE FLOOR

Mr. HARKIN. Mr. President, I ask unanimous consent that the following fellow and interns be granted floor privileges for the remainder of the day: Bryan Boroughs, Lucy Stein, Shauna Agan, Douglas Dorando, Keagan Buchanan, and Andrea Jarcho.

The ACTING PRESIDENT pro tempore. Without objection, it is so ordered.

Mr. BROWN of Ohio. Mr. President, I ask unanimous consent that the privilege of the floor be granted to Ben Cohen, a fellow on my staff.

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

NATIONAL WORK AND FAMILY MONTH

Mr. BROWN of Ohio. Madam President, I ask unanimous consent that the Senate proceed to S. Res. 533 submitted earlier today.

The PRESIDING OFFICER. The clerk will report the resolution by title.

The legislative clerk read as follows:

A resolution (S. Res. 533) designating October 2012 as ''National Work and Family Month.''

There being no objection, the Senate proceeded to consider the resolution.

Mr. BROWN of Ohio. I ask unanimous consent that the 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 any statements be printed in the RECORD.

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

The resolution (S. Res. 533) was agreed to.

The preamble was agreed to.

The resolution, with its preamble, reads as follows:

S. RES. 533

Whereas, according to a report by WorldatWork, a nonprofit professional association with expertise in attracting, motivating, and retaining employees, the quality of workers' jobs and the supportiveness of the workplace of the workers are key predictors of the job productivity, job satisfaction, and commitment to the employer of those workers, as well as of the ability of the employer to retain those workers;

Whereas ''work-life balance'' refers to specific organizational practices, policies, and programs that are guided by a philosophy of active support for the efforts of employees to achieve success within and outside the workplace, such as caring for dependents, health and wellness, paid and unpaid time off, financial support, community involvement, and workplace culture;

Whereas numerous studies show that employers that offer effective work-life balance programs are better able to recruit more talented employees, maintain a happier, healthier, and less stressed workforce, and retain experienced employees, which produces a more productive and stable workforce with less voluntary turnover;

Whereas job flexibility often allows parents to be more involved in the lives of their children, and research demonstrates that parental involvement is associated with higher achievement in language and mathematics, improved behavior, greater academic persistence, and lower dropout rates in children;

Whereas military families have special work-family needs that often require robust

policies and programs that provide flexibility to employees in unique circumstances;

Whereas studies report that family rituals, such as sitting down to dinner together and sharing activities on weekends and holidays, positively influence the health and development of children and that children who eat dinner with their families every day consume nearly a full serving more of fruits and vegetables per day than those who never eat dinner with their families or do so only occasionally; and

Whereas the month of October is an appropriate month to designate as National Work and Family Month: Now, therefore, be it

Resolved, That the Senate—

(1) designates October 2012 as ''National Work and Family Month'';

(2) recognizes the importance of work schedules that allow employees to spend time with their families to job productivity and healthy families;

(3) urges public officials, employers, employees, and the general public to work together to achieve more balance between work and family; and

(4) calls upon the people of the United States to observe National Work and Family Month with appropriate ceremonies and activities.

MEASURES READ THE 1ST TIME—S. 3457 AND H.R. 4078

Mr. BROWN of Ohio. Madam President, I understand there are two bills at the desk, and I ask for their first reading en bloc.

The PRESIDING OFFICER. The clerk will read the bills by title for the first time.

The legislative clerk read as follows:

A bill (S. 3457) to require the Secretary of Veterans Affairs to establish a veterans job corps, and for other purposes.

A bill (H.R. 4078) to provide that no agency may take any significant regulatory action until the unemployment rate is equal to or less than 6.0 percent.

Mr. BROWN of Ohio. I now ask for a second reading en bloc and object to my own request en bloc.

The PRESIDING OFFICER. Objection having been heard, the bills will be read for a second time on the next legislative day.

ORDERS FOR TUESDAY, JULY 31, 2012

Mr. BROWN of Ohio. Madam President, I ask unanimous consent that when the Senate completes its business today, it adjourn until 10 a.m. on Tuesday, July 31; 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 the time until 12:30 p.m. be equally divided and controlled between the two leaders or their designees, with the majority controlling the first hour and the Republicans controlling the second hour; and that the Senate recess from 12:30 p.m. until 2:15 p.m. to allow for the weekly caucus meetings.

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

PROGRAM

Mr. BROWN of Ohio. Madam President, we will continue to debate the cybersecurity bill tomorrow. Senators will be notified when votes are scheduled.

ADJOURNMENT UNTIL 10 A.M. TOMORROW

Mr. BROWN of Ohio. If there is no further business to come before the Senate, I ask unanimous consent that the Senate adjourn under the previous order.

There being no objection, the Senate, at 6:51 p.m., adjourned until Tuesday, July 31, 2012, at 10 a.m.