Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 National Security Strategy - § 21 references coded [ 1.35% Coverage]

Reference 1 - 0.04% Coverage

our efforts to shape an international order that promotes a just peace must facilitate cooperation capable of addressing the problems of our time

Reference 2 - 0.04% Coverage

For instance, we pursue close and regular collaboration with our close allies the United Kingdom, France, and Germany on issues of mutual and global concern.

Reference 3 - 0.04% Coverage

Swift and effective international action often turns on the political will of coalitions of countries that comprise regional or international institutions.

Reference 4 - 0.04% Coverage

seeking common ground. Diplomats, development experts, and others in the United States Government must be able to work side by side to support a common agenda.

Reference 5 - 0.05% Coverage

Such partnerships are critical to U.S. success at home and abroad, and we will support them through enhanced opportunities for engagement, coordination, transparency, and information sharing.

Reference 6 - 0.08% Coverage

Thus, we are working with partners abroad to confront threats that often begin beyond our borders. And we are developing lines of coordination at home across Federal, state, local, tribal, territorial, nongovernmental, and private-sector partners, as well as individuals and communities.

Reference 7 - 0.06% Coverage

We are improving information sharing and cooperation by linking networks to facilitate Federal, state, and local capabilities to seamlessly exchange messages and information, conduct searches, and collaborate.

Reference 8 - 0.03% Coverage

We are coordinating better with foreign partners to identify, track, limit access to funding, and prevent terrorist travel.

Reference 9 - 0.06% Coverage

Recognizing the inextricable link between domestic and transnational security, we will collaborate bilaterally, regionally, and through international institutions to promote global efforts to prevent terrorist attacks.

Reference 10 - 0.07% Coverage

designing appropriate assistance strategies and will facilitate the kind of collaboration that is essential—within our government and with international organizations—in those instances when we engage in the difficult work of helping to bring conflicts to an end.

Reference 11 - 0.06% Coverage

This requires investing now in the capable partners of the future; building today the capacity to strengthen the foundations of our common security, and modernizing our capabilities in order to ensure that we are agile in the face of change

Reference 12 - 0.06% Coverage

We will work with all the key players— including all levels of government and the private sector, nationally and internationally—to investigate cyber intrusion and to ensure an organized and unified response to future cyber incidents

Reference 13 - 0.15% Coverage

We must reinvigorate and fortify it for the 21st century: by preventing cycles of boom and bust with new rules of the road at home and abroad; by saving more and spending less; by resisting protectionism and promoting trade that is free and fair; by coordinating our actions with other countries, and reforming international institutions to give emerging economies a greater voice and greater responsibility; and by supporting development that promotes good governance, unleashes the potential of different populations, and creates new markets overseas.

Reference 14 - 0.10% Coverage

Our strategy to attack these networks must respond in kind and target their illicit resources and access to the global financial system through financial measures, administration and enforcement of regulatory authorities, outreach to the private sector and our foreign partners, and collaboration on international standards and information sharing.

Reference 15 - 0.04% Coverage

We are working closely with citizens, communities, and political and civil society leaders to strengthen key institutions of democratic accountability

Reference 16 - 0.06% Coverage

those nations that defy international norms or fail to meet their sovereign responsibilities will be denied the incentives that come with greater integration and collaboration with the international community

Reference 17 - 0.07% Coverage

Pursue Decisions though a Wide Range of Frameworks and Coalitions: We need to spur and harness a new diversity of instruments, alliances, and institutions in which a division of labor emerges on the basis of effectiveness, competency, and long-term reliability.

Reference 18 - 0.07% Coverage

This requires enhanced coordination among the United Nations, regional organizations, international financial institutions, specialized agencies, and other actors that are better placed or equipped to manage certain threats and challenges.

Reference 19 - 0.10% Coverage

While we are pursuing G-8 initiatives with proven and long-standing partners, have begun to shift the focus of our economic coordination to the G-20, which is more reflective of today’s diffusion of power and the need to enlist the efforts of a broader spectrum of countries across Asia to Europe, Africa to the Middle East, and our neighbors in the Americas.

Reference 20 - 0.05% Coverage

Addressing these transnational risks requires advance preparation, extensive collaboration with the global community, and the development of a resilient population at home.

Reference 21 - 0.07% Coverage

We are enhancing international collaboration and strengthening multilateral institutions in order to improve global surveillance and early warning capabilities and quickly enact control and containment measures against the next pandemic threat

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 Quadrennial Defense Review - § 4 references coded [ 0.07% Coverage]

Reference 1 - 0.02% Coverage

Achieving the Department’s strategic objectives requires close collaboration with counterparts

Reference 2 - 0.02% Coverage

Effective strategic communication requires close collaboration across interagency lines at all stages,

Reference 3 - 0.01% Coverage

outline a common vision of interagency collaboration

Reference 4 - 0.02% Coverage

Achieving the Department’s strategic objectives requires close collaboration with key counterparts at home and with allies and partners abroad.

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 DoD Cyber Strategy - § 5 references coded [ 1.11% Coverage]

Reference 1 - 0.06% Coverage

The Internet was designed to be collaborative,

Reference 2 - 0.26% Coverage

An example of one critical initiative is the 2010 memorandum of agreement signed by the Secretary of Defense and Secretary of Homeland Security to align and enhance cybersecurity collaboration.

Reference 3 - 0.26% Coverage

Given the rapid pace of change that characterizes cyberspace, DoD will continue to work with interagency partners and the private sector to examine new collaborative approaches to cybersecurity.

Reference 4 - 0.21% Coverage

A collaborative national effort will develop common and workable solutions to policy problems that both increase cybersecurity and further the public good.

Reference 5 - 0.33% Coverage

In support of the U.S. International Strategy for Cyberspace and in collaboration with its interagency partners, DoD will seek increasingly robust international relationships to reflect our core commitments and common interests in cyberspace.

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 International Strategy for Cyberspace - § 31 references coded [ 4.43% Coverage]

Reference 1 - 0.14% Coverage

New technologies improving agriculture or promoting public health are shared with those in greatest need, and difficult problems benefit from global collaboration among experts and innovators~

Reference 2 - 0.11% Coverage

When a crime is committed internationally, law enforcement agencies are able to collaborate to safeguard and share evidence and bring individuals to justice~

Reference 3 - 0.16% Coverage

They continue to collaborate bilaterally, multilaterally, and internationally to bring more of the world into the information age and into the consensus of states that seek to preserve the Internet and its core characteristics~

Reference 4 - 0.08% Coverage

To sustain this environment, international collaboration is more than a best practice; it is a first principle~

Reference 5 - 0.12% Coverage

An effective strategy will require action on many fronts, with shared responsibility at every level of society, from the end-user up through collaboration among nation-states~

Reference 6 - 0.11% Coverage

Finally, incident response will require increased collaboration and technical information sharing with the private sector and international community~

Reference 7 - 0.07% Coverage

These efforts will be supported by meaningful collaboration with the private sector at home and abroad~

Reference 8 - 0.12% Coverage

Bilateral and Multilateral Partnerships~ We will work bilaterally with nations to build collaboration on cyberspace issues important to our governments and our peoples~

Reference 9 - 0.17% Coverage

Private Sector Collaboration~ Although the private sector already plays an important role in international and multi-stakeholder organizations, we will continue to leverage existing partnership mechanisms to engage with industry partners~

Reference 10 - 0.15% Coverage

Ensuring the resilience of our networks and information systems requires collective and concerted national action that spans the whole of government, in collaboration with the private sector and individual citizens~

Reference 11 - 0.13% Coverage

Today, through existing and developing collaborations in the technical and military defense arenas, nations share an unprecedented ability to recognize and respond to incidents

Reference 12 - 0.13% Coverage

The United States has a shared interest in assisting less developed nations to build capacity for defense, and in collaboration with our partners, will intensify our focus on this area~

Reference 13 - 0.27% Coverage

International information infrastructures continue to mature and expand, providing more nations with the opportunity to access the global flow of information~ The growth of the networks worldwide, and expansion of access to them, enriches the world community, yet also presents new challenges and opportunities for collaboration on issues of traditional and cybersecurity~

Reference 14 - 0.16% Coverage

As countries develop a stake in cyberspace issues, we intend our dialogues to mature from capacity-building to active economic, technical, law enforcement, defense and diplomatic collaboration on issues of mutual concern~

Reference 15 - 0.21% Coverage

To fully realize this future in which cyberspace lives up to its potential for all, the United States Government organizes its activities across seven interdependent areas of activity, each demanding collaboration within our government, with international partners, and with the private sector~

Reference 16 - 0.13% Coverage

The United States will foster collaboration between the public and private sector to ensure the promulgation of international standards-based requirements for products and services~

Reference 17 - 0.12% Coverage

We will also look to fora that enable multi-stakeholder collaboration and consensus building, to further elaborate the Internet policy principles outlined in this document~

Reference 18 - 0.25% Coverage

Agencies across the United States Government are collaborating, together with the private sector, to protect innovation from industrial espionage, to protect Federal, state, and local government networks, to protect military operations from degraded operating environments, and to secure critical infrastructure against intrusions and attacks

Reference 19 - 0.13% Coverage

No one nation can have full insight into the world’s networks; we have an obligation to share our insights about our own networks and collaborate with others when events might threaten us all~

Reference 20 - 0.07% Coverage

We will expand these capabilities through international collaboration to enhance overall resilience~

Reference 21 - 0.04% Coverage

Law Enforcement: Extending Collaboration and the Rule of Law

Reference 22 - 0.24% Coverage

The United States and our allies regularly depend upon cooperation and assistance from other countries when investigating and prosecuting cybercrime cases~ This cooperation is most effective and meaningful when the countries have common cybercrime laws, which facilitates evidence-sharing, extradition, and other types of coordination~

Reference 23 - 0.20% Coverage

As the United States and our partners engage in dialogue and help build capacity among law enforcement organizations worldwide, we will integrate this approach, uniting protection of privacy, fundamental freedoms, and innovation with collaboration to combat crimes in cyberspace~

Reference 24 - 0.20% Coverage

By developing a shared understanding of standard operating procedures, our armed forces can enhance security through coordination and greater information exchange; these engagements will diminish misperceptions about military activities and the potential for escalatory behavior~

Reference 25 - 0.14% Coverage

The United States recognizes that the effective coordination of these resources has facilitated the Internet’s success, and will continue to support those effective, multi-stakeholder processes~

Reference 26 - 0.15% Coverage

The United States will expand these collaborations, work in-country to support private-sector investment in capacity, draw attention to this critical need, and work to build new collaborations in the coming years~

Reference 27 - 0.16% Coverage

The United States will continue to identify, develop, and refine best practices and technical standards in collaboration and close partnership with industry, and will expand our efforts to promote awareness of and access to them~

Reference 28 - 0.09% Coverage

We will further promote collaborative science and technology research to enhance cybersecurity tools and capabilities~

Reference 29 - 0.14% Coverage

Criminal threats can originate from any connected country, and many countries need substantial help in developing the investigative capacities required to collaborate in such investigations~

Reference 30 - 0.12% Coverage

We have taken a lead role in convening fora, such as the Meridian Conference, which fosters collaboration on critical information infrastructure protection issues~

Reference 31 - 0.11% Coverage

Collaborate with civil society and nongovernment organizations to establish safeguards protecting their Internet activity from unlawful digital intrusions.

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 National Military Strategy - § 4 references coded [ 0.54% Coverage]

Reference 1 - 0.16% Coverage

We will nest our efforts to build partner capacity with broader national security priorities, consolidate our institutional processes, and improve coordination across agencies.

Reference 2 - 0.19% Coverage

Strategic Command and Cyber Command will collaborate with U.S. government agencies, nongovernment entities, industry, and international actors to develop new cyber norms, capabilities, organizations, and skills.

Reference 3 - 0.13% Coverage

Efforts to disrupt illicit trafficking sources and transit zones must be coordinated across North, Central and South America, and the Caribbean.

Reference 4 - 0.06% Coverage

Preparation is indispensable when conditions demand collaboration.

Files\\2011 Case Study\\CS1\_Secondary Sources\_Authoritative\\2009 Cyberspace Policy Review Assuring a Trusted and R - § 23 references coded [ 0.47% Coverage]

Reference 1 - 0.01% Coverage

ent   
9.   
In collaboration with other EOP enti

Reference 2 - 0.01% Coverage

suggest areas of improvement or collaboration

Reference 3 - 0.01% Coverage

opportunities to improve collaboration.

Reference 4 - 0.01% Coverage

collaboration

Reference 5 - 0.01% Coverage

collaborative

Reference 6 - 0.01% Coverage

collaboratively

Reference 7 - 0.05% Coverage

In addition, the Federal government—continuing the long-term history of collaboration with the private sector—should develop a proactive engagement plan for use with international standards bodies.

Reference 8 - 0.04% Coverage

New agreements between governments and industry may need to be documented to enable international information sharing as well as strategic and operational collaboration

Reference 9 - 0.02% Coverage

in collaboration with State, local, and tribal governments and industry

Reference 10 - 0.02% Coverage

in collaboration with industry and the civil liberties and privacy community

Reference 11 - 0.03% Coverage

International collaboration makes effective government-private sector collaboration in the United States more challenging.

Reference 12 - 0.01% Coverage

collaboration

Reference 13 - 0.01% Coverage

collaboration

Reference 14 - 0.02% Coverage

encouragement of collaboration between academic and industrial laboratories

Reference 15 - 0.02% Coverage

in collaboration with the private sector and other stakeholders

Reference 16 - 0.03% Coverage

The Federal government—in collaboration with industry and the civil liberties and privacy communities—

Reference 17 - 0.07% Coverage

In collaboration with other EOP entities, develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure;

Reference 18 - 0.05% Coverage

Encourage collaboration between academic and industrial laboratories to develop migration paths and incentives for the rapid adoption of research and technology development innovations

Reference 19 - 0.01% Coverage

suggest areas of improvement or collaboration

Reference 20 - 0.01% Coverage

the government must foster an environment for collaboration

Reference 21 - 0.01% Coverage

opportunities for collaboration between agencies

Reference 22 - 0.01% Coverage

required NIST to collaborate with NSA

Reference 23 - 0.04% Coverage

Following on this research, international packet switching network standards were developed in collaboration with entities in other countries under the auspices of the ITU

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2014 Quadrennial Defense Review - § 1 reference coded [ 0.05% Coverage]

Reference 1 - 0.05% Coverage

With our allies and partners, we will make greater efforts to coordinate our planning to optimize their contributions to their own security and to our many combined activities.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 12 references coded [ 1.18% Coverage]

Reference 1 - 0.14% Coverage

Information sharing and interagency coordination. To secure and advance U.S. interests in cyberspace, DoD seeks to share information and coordinate with U.S. government agencies in an integrated fashion on a range of cyber activities.

Reference 2 - 0.02% Coverage

Build bridges to the private sector.

Reference 3 - 0.08% Coverage

Going forward, DoD will work closely with the private sector to validate and commercialize new ideas for cybersecurity for the Department.

Reference 4 - 0.12% Coverage

The Defense Department requires the commitment and coordination of multiple leaders and communities across DoD and the broader U.S. government to carry out its missions and execute this strategy.

Reference 5 - 0.14% Coverage

This strategy recognizes that effective cybersecurity will require close collaboration within DoD and across the federal government, with industry, with international allies and partners, and with state and local governments.

Reference 6 - 0.08% Coverage

For each of DoD’s missions, DoD must continue to develop routine relationships and processes for coordinating its cyber operations.

Reference 7 - 0.09% Coverage

The Defense Department will continue to collaborate closely with the private sector and other agencies of the U.S. government to strengthen attribution.

Reference 8 - 0.06% Coverage

All three of DoD’s cyber missions require close collaboration with foreign allies and partners.

Reference 9 - 0.11% Coverage

Build collaboration between the acquisition, intelligence, counterintelligence, law enforcement, and operations communities to prevent, mitigate, and respond to data loss.

Reference 10 - 0.20% Coverage

The strategy will specify how DoD’s counterintelligence agencies will collaborate more effectively with the broader U.S. intelligence and law enforcement communities on investigations and human and technical operations to thwart cyber-enabled intellectual property theft against the United States and its allies and partners.

Reference 11 - 0.06% Coverage

assessment of our mutual cyber defense posture, and collaborative approaches to building cyber expertise.

Reference 12 - 0.09% Coverage

Success requires close collaboration across DoD, between agencies of the U.S. government, with the private sector, and with U.S. allies and partners.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Military Strategy - § 12 references coded [ 1.84% Coverage]

Reference 1 - 0.11% Coverage

Concurrently, we are leading multiple coalition efforts to disrupt, degrade, and defeat VEOs.

Reference 2 - 0.20% Coverage

each pose serious security concerns which the international community is working to collectively address by way of common policies, shared messages, and coordinated action.

Reference 3 - 0.01% Coverage

coordinate,

Reference 4 - 0.14% Coverage

Hybrid conflicts serve to increase ambiguity, complicate decision-making, and slow the coordination of effective responses.

Reference 5 - 0.13% Coverage

militarily sustainable manner that optimizes the power of coalitions, as we are demonstrating in Afghanistan and Iraq.

Reference 6 - 0.18% Coverage

Similarly, in Iraq a broad coalition of over 60 nations is providing security assistance, training, airlift, and strike support in its struggle against ISIL.

Reference 7 - 0.23% Coverage

Thus counter-VEO campaigns demand that our military, in close coordination with other U.S. agencies and international organizations, assist local governments in addressing the root causes of conflict.

Reference 8 - 0.20% Coverage

Through such activities, we coordinate with other U.S. agencies and mission partners to build cultural awareness and affirm relationships that increase regional stability.

Reference 9 - 0.16% Coverage

The best   
way to counter VEOs is by way of sustained pressure using local forces augmented by specialized U.S. and coalition military strengths

Reference 10 - 0.10% Coverage

Counterterrorism operations also involve coordinated efforts with other U.S. agencies

Reference 11 - 0.18% Coverage

The U.S. military also remains   
ready to conduct limited stability operations when required, working with interagency, coalition, and host-nation forces.

Reference 12 - 0.20% Coverage

Additionally, we are more fully coordinating requirements, plans, and operational execution at home and abroad to maximize collective capabilities against common concerns.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Security Strategy - § 10 references coded [ 0.94% Coverage]

Reference 1 - 0.10% Coverage

We led a multinational coalition to support the Afghan government to take responsibility for the security of their country, while supporting Afghanistan’s first peaceful, democratic transition of power.

Reference 2 - 0.06% Coverage

mobilizing the international community to meet the urgent challenges posed by climate change and infectious disease.

Reference 3 - 0.10% Coverage

It also requires international support, which is why we are leading an unprecedented international coalition to work with the Iraqi government and strengthen its military to regain sovereignty.

Reference 4 - 0.12% Coverage

We will also keep our edge by opening our national labs to more commercial partnerships while tapping research and development in the private sector, including a wide range of start-ups and firms at the leading edge of America’s innovation economy.

Reference 5 - 0.13% Coverage

At the same time, we will keep the door open to greater collaboration with Russia in areas of common interests, should it choose a different path—a path of peaceful cooperation that respects the sovereignty and democratic development of neighboring states.

Reference 6 - 0.08% Coverage

We will work with the U.N. and our Arab and European partners in an effort to help stabilize Libya and reduce the threat posed by lawless militias and extremists.

Reference 7 - 0.13% Coverage

We are expanding our collaboration across the Americas to support democratic consolidation and increase public-private partnerships in education, sustainable development, access to electricity, climate resilience, and countering transnational organized crime.

Reference 8 - 0.09% Coverage

Such collaboration is especially important in vulnerable countries like Guatemala, El Salvador, and Honduras, where government institutions are threatened by criminal syndicates.

Reference 9 - 0.06% Coverage

We will continue to collaborate with established and emerging powers to promote our shared security and defend our common humanity

Reference 10 - 0.06% Coverage

We will uphold and refresh the international rules and norms that set the parameters for such collaboration and competition.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 14 references coded [ 2.82% Coverage]

Reference 1 - 0.17% Coverage

To strengthen collective network defenses, the United States Government collaborates with the private sector to identify key systems that must be protected and to implement best practices in cybersecurity.

Reference 2 - 0.25% Coverage

This collaboration and research identified a small subset of entities in several critical infrastructure sectors where a cybersecurity incident and its second or third-order effects could result in catastrophic regional or national effects on public health or safety, economic security, or national security.

Reference 3 - 0.13% Coverage

This public-private collaboration is also shaping the government’s planning, mitigation, and response efforts in the event of significant cyber incidents.

Reference 4 - 0.24% Coverage

The Cross-Agency Priority goal framework was established by the GPRA Modernization Act of 2010 and is used to accelerate progress on a limited number of Presidential priority areas where implementation will require collaboration and coordinated action by multiple departments and agencies.

Reference 5 - 0.26% Coverage

The United States Government is making a renewed push to increase the number of parties to the Budapest Convention, and to increase the membership of the 24/7 Network for law enforcement points of contact. Fifty-three countries have signed the Budapest Convention with forty-four of those ratifying it into domestic law.

Reference 6 - 0.17% Coverage

In addition, the Administration has put in place mechanisms that ensure departments and agencies are combining their capabilities and resources into effective, coordinated responses to malicious cyber activity.

Reference 7 - 0.31% Coverage

As one example, in 2014, the White House began using the Cyber Response Group, or CRG—modeled on the highly effective and long-standing Counterterrorism Security Group—to handle certain incident response coordination tasks. The CRG focuses on sharing threat information, malware signatures, plans of state and non-state actors, and coordinating responses across the government.

Reference 8 - 0.11% Coverage

Administration views forums for agile interagency coordination, like the CRG as a linchpin in the government’s response capabilities.

Reference 9 - 0.12% Coverage

Administration seeks to share knowledge about ongoing threats and attacks and coordinate all elements of the government’s response at the highest levels.

Reference 10 - 0.30% Coverage

In taking this “whole of government” approach, the Administration is working to establish clear lanes of responsibility for Federal departments and agencies, build the communications channels necessary for near real-time situational awareness, and bolster government engagement with the private sector so that companies know whom to contact when faced with a cyber threat.

Reference 11 - 0.20% Coverage

To that end, the whole-of-government consultative process, constant collaboration with the private sector, and international coordination all increase the likelihood that the signaling component of the U.S. deterrent effort is successful.

Reference 12 - 0.27% Coverage

Effective international collaboration on cyber deterrence will require the United States to share its perspective on the threat environment with allies and international partners, lead the way in developing and promulgating norms of state behavior in cyberspace, and support international partners’ efforts to secure their own networks.

Reference 13 - 0.15% Coverage

DHS and the FBI regularly work with their international partners to share information on incidents of concern and, when appropriate, work together to investigate and mitigate incidents.

Reference 14 - 0.14% Coverage

One example of such efforts is the United States Government’s collaboration with the private sector on implementing the National Strategy for Trusted Identities in Cyberspace

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2017 National Security Strategy - § 9 references coded [ 0.49% Coverage]

Reference 1 - 0.06% Coverage

In accordance with the protection of civil liberties and privacy, the U.S. Government will expand collaboration with the private sector so that we can bett er detect and att ribute att acks.

Reference 2 - 0.05% Coverage

Agencies from all levels of government must coordinate bett er and apply lessons learned from exercises to pinpoint the areas and capabilities that require improvement.

Reference 3 - 0.09% Coverage

To improve the coordination among the private sector and all levels of government that is needed to improve resilience, we must make a stronger commitment to protecting sensitive information so that all partners actively identify and share vulnerabilities and work collaboratively to reduce them.

Reference 4 - 0.07% Coverage

We will nurture a healthy innovation economy that collaborates with allies and partners, improves STEM education, draws on an advanced technical workforce, and invests in early-stage research and development (R&D).

Reference 5 - 0.04% Coverage

The U.S. Government must improve our collaboration with industry and academia and our recruitment of technical talent.

Reference 6 - 0.07% Coverage

In the ongoing contest s for power, our diplomats must build and lead coalitions that advance shared interest s and art iculate America’s vision in international forums, in bilateral   
relationships, and at local levels within states.

Reference 7 - 0.03% Coverage

Repressive leaders often collaborate to subvert free societies and corrupt multilateral organizations.

Reference 8 - 0.03% Coverage

We will prioritize collaboration with aspiring partners that are aligned with U.S. interests.

Reference 9 - 0.06% Coverage

Th e United States will deepen collaboration with our European allies and partners to confront forces threatening to undermine our common values, security interests, and shared vision.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 DoD Cyber Strategy Summary - § 4 references coded [ 2.11% Coverage]

Reference 1 - 0.29% Coverage

We will collaborate with our interagency, industry, and international partners to advance our mutual interests.

Reference 2 - 0.52% Coverage

We will defend forward to halt or degrade cyberspace operations targeting the Department, and we will collaborate to strengthen the cybersecurity and resilience of DoD, DCI, and DIB networks and systems.

Reference 3 - 0.49% Coverage

The Department also provides public and private sector partners with indications and warning (I&W) of malicious cyber activity, in coordination with other Federal departments and agencies.

Reference 4 - 0.81% Coverage

In coordination with other Federal departments and agencies, the Department will build trusted relationships with private sector entities that are critical enablers of military operations and carry out deliberate planning and collaborative training that enables mutually supporting cybersecurity activities.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Cyber Strategy - § 15 references coded [ 2.97% Coverage]

Reference 1 - 0.13% Coverage

It will require a series of coordinated actions focused on protecting government networks, protecting critical infrastructure, and combating cybercrime.

Reference 2 - 0.17% Coverage

It will also identify   
and bridge existing gaps in responsibilities and coordination among Federal and non-Federal incident response efforts and promote more routine training, exercises, and coordination.

Reference 3 - 0.15% Coverage

The Federal Government will continue to coordinate the development of cybersecurity standards and guidance to safeguard the electoral process and the tools that deliver a secure system.

Reference 4 - 0.38% Coverage

Given the criticality of maritime transportation to the United States and global economy and the minimal risk-reduction investments to protect against cyber exploitation made thus far, the United States will move quickly to clarify maritime cybersecurity roles and responsibilities; promote enhanced mechanisms for international coordination and information sharing; and accelerate the development of next-generation cyber-resilient maritime infrastructure.

Reference 5 - 0.18% Coverage

The United States will also lead in developing interoperable and mutually beneficial systems to encourage efficient cross-border   
information exchange for law   
enforcement purposes and reduce barriers to coordination.

Reference 6 - 0.30% Coverage

Finally, the Administration will collaborate with international partners to promote open, industry-driven standards with government support, as appropriate, and risk-based approaches to address cybersecurity challenges to include platform and managed service approaches that lower barriers to secure practice adoption across the breadth of the ecosystem.

Reference 7 - 0.20% Coverage

We will collaborate with the private sector and civil society to understand trends in technology advancement to maintain the United States technological edge in connected technologies and to ensure secure practices are adopted from the outset.

Reference 8 - 0.16% Coverage

This includes promotion and use of coordinated vulnerability disclosure, crowd-sourced testing, and other innovative assessments that improve resiliency ahead of exploitation or attack.

Reference 9 - 0.30% Coverage

The United States Government will also leverage publicprivate collaboration to develop and circulate the NICE Framework, which provides a standardized approach for identifying cybersecurity workforce gaps, while also implementing actions to prepare, grow, and sustain a workforce that can defend and bolster America’s critical   
infrastructure and innovation base.

Reference 10 - 0.04% Coverage

LEAD WITH OBJECTIVE, COLLABORATIVE INTELLIGENCE:

Reference 11 - 0.16% Coverage

BUILD A CYBER DETERRENCE INITIATIVE: The imposition of consequences will be more impactful and send a stronger message if it is carried out in concert with a broader coalition of like-minded states.

Reference 12 - 0.18% Coverage

The United States will launch an international Cyber Deterrence Initiative to build such a coalition and develop tailored strategies to ensure adversaries understand the consequences of their malicious cyber behavior.

Reference 13 - 0.28% Coverage

The United States will work with like-minded states to coordinate and support each other’s responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken, and joint imposition of consequences against malign actors.

Reference 14 - 0.19% Coverage

Collaboration with allies and partners is also essential to ensure we can continue to benefit from the cross-border communications, content creation, and commerce generated by the open, interoperable architecture of the Internet.

Reference 15 - 0.15% Coverage

We will also aggressively expand efforts to share automated and actionable cyber threat information, enhance cybersecurity coordination, and promote analytical and technical exchanges.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Defense Strategy Summary - § 3 references coded [ 0.95% Coverage]

Reference 1 - 0.36% Coverage

There is a positive side to this as well, as our partners in sustaining security are also more than just nation-states: multilateral organizations, non-governmental organizations, corporations, and strategic influencers provide opportunities for collaboration and partnership.

Reference 2 - 0.24% Coverage

Expand regional consultative mechanisms and collaborative planning. We will develop new partnerships around shared interests to reinforce regional coalitions and security cooperation.

Reference 3 - 0.34% Coverage

Form enduring coalitions in the Middle East. We will foster a stable and secure Middle East that denies safe havens for terrorists, is not dominated by any power hostile to the United States, and that contributes to stable global energy markets and secure trade routes.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Defense Strategy - § 21 references coded [ 1.40% Coverage]

Reference 1 - 0.09% Coverage

The NDS further explains how we will collaborate with our NATO Allies and partners to reinforce robust deterrence in the face of Russian aggression while mitigating and protecting against threats from North Korea, Iran, violent extremist organizations, and transboundary challenges such as climate change.

Reference 2 - 0.07% Coverage

Integrated deterrence means using every tool at the Department’s disposal, in close collaboration with our counterparts across the U.S. Government and with Allies and partners, to ensure that potential foes understand the folly of aggression.

Reference 3 - 0.05% Coverage

Tailored to specific circumstances, it applies a coordinated, multifaceted approach to reducing competitors’ perceptions of the net benefits of aggression relative to restraint.

Reference 4 - 0.04% Coverage

The 2022 NDS advances a strategy focused on the PRC and on collaboration with our growing network of Allies and partners on common objectives.

Reference 5 - 0.09% Coverage

We will strengthen major regional security architectures with our Allies and partners based on complementary contributions; combined, collaborative operations and force planning; increased intelligence and information sharing; new operational concepts; and our ability to draw on the Joint Force worldwide.

Reference 6 - 0.07% Coverage

Integrated deterrence is how we will align the Department’s policies, investments, and activities to sustain and strengthen deterrence – tailored to specific competitors and coordinated to maximum effect inside and outside the Department.

Reference 7 - 0.07% Coverage

Through close collaboration with U.S. Government departments and agencies and with our Allies and partners, we will diversify our posture and broaden the scope of cooperation, adding complexity to competitors’ military planning and execution.

Reference 8 - 0.06% Coverage

Our work will prioritize closer coordination with U.S. interagency, state, local, tribal, and territorial partners, as well as with the private sector, starting with the defense industrial base.

Reference 9 - 0.07% Coverage

Collaboration with Allies and partners will cement joint capability with the aid of multilateral exercises, codevelopment of technologies, greater intelligence and information sharing, and combined planning for shared deterrence challenges.

Reference 10 - 0.10% Coverage

Deterring North Korean Attacks. The Department will continue to deter attacks through forward posture; integrated air and missile defense; close coordination and interoperability with our ROK Ally; nuclear deterrence; resilience initiatives; and the potential for direct cost imposition approaches that come from globally deployable Joint Forces.

Reference 11 - 0.09% Coverage

Deterring Iranian Attacks. To deter large-scale Iranian attacks on vital national security interests and partners in the region, the Department will work to increase partner capability and resilience, particularly in air and missile defense, while collaborating with partners to expose Iranian gray zone operations.

Reference 12 - 0.04% Coverage

In the Indo-Pacific, we will continue key infrastructure investments and coordinate with the Department of State to expand access in the region.

Reference 13 - 0.05% Coverage

Early and continuous consideration, engagement, and, where possible, collaboration with Allies and partners in planning is essential for advancing our shared interests.

Reference 14 - 0.06% Coverage

To strengthen and sustain deterrence, the Department will prioritize interoperability and enable coalitions with enhanced capabilities, new operating concepts, and combined, collaborative force planning.

Reference 15 - 0.04% Coverage

We will consult and coordinate with Allies and partners as we modernize our nuclear forces, reinforcing our extended deterrence commitments.

Reference 16 - 0.09% Coverage

The Department will collaborate with Allies and partners to build capacity along Europe’s eastern flank, strengthening defensive antiarea/access-denial capabilities and indications and warning; expanding readiness, training, and exercises; and promoting resilience, including against hybrid and cyber actions.

Reference 17 - 0.04% Coverage

As in all regions, the Department will work collaboratively, seeking to understand our partners’ security needs and areas of mutual concern.

Reference 18 - 0.09% Coverage

We will orient our approach on the continent towards security cooperation; increase coordination with Allies, multilateral organizations, and regional bodies that share these objectives; and support U.S. interagency initiatives in the region, including efforts to disrupt malign PRC and Russian activities on the continent.

Reference 19 - 0.07% Coverage

These include coordination with and contributions of Allies and partners, deterrent effects of U.S. nuclear posture, and leveraging posture and capabilities not solely engaged in the primary warfight – for example, cyber and space.

Reference 20 - 0.07% Coverage

To preserve command, control, and communications in a fast-paced battlefield, we will make our network architectures more resilient against system-level exploitation and disruption so as to ensure effective coordination of distributed forces.

Reference 21 - 0.05% Coverage

Working in service of the American people, and in collaboration with our partners around the world, the men and women of our superbly capable Joint Force stand ready to do so again.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Military Strategy - § 1 reference coded [ 1.04% Coverage]

Reference 1 - 1.04% Coverage

7. STRENGTHEN RELATIONSHIPS WITH ALLIES AND PARTNERS Seek opportunities to collaborate and improve interoperability with allies and partners to confront enduring and emerging challenges. Foster strong relationships now — because we cannot surge trust in crisis.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Security Strategy - § 24 references coded [ 1.68% Coverage]

Reference 1 - 0.06% Coverage

We are securing our supply chains, including through new forms of public-private collaboration, and using public procurement in critical markets to stimulate demand for innovation.

Reference 2 - 0.04% Coverage

We will help construct and preserve coalitions that engage all of these countries and leverage their collective strengths.

Reference 3 - 0.04% Coverage

Incorporating allies and partners at every stage of defense planning is crucial to meaningful collaboration.

Reference 4 - 0.07% Coverage

We also seek to remove barriers to deeper collaboration with allies and partners, to include issues related to joint capability development and production to safeguard our shared military-technological edge.

Reference 5 - 0.06% Coverage

Integration with allies and partners through investments in interoperability and joint capability development, cooperative posture planning, and coordinated diplomatic and economic approaches.

Reference 6 - 0.07% Coverage

Integrated deterrence requires us to more effectively coordinate, network, and innovate so that any competitor thinking about pressing for advantage in one domain understands that we can respond in many others as well.

Reference 7 - 0.05% Coverage

Working with a broad and durable international coalition, we have marshalled near-record levels of security assistance to ensure Ukraine has the means to defend itself.

Reference 8 - 0.03% Coverage

And we will rally the world to hold Russia accountable for the atrocities they have unleashed across Ukraine.

Reference 9 - 0.12% Coverage

Through collaborative work in the International Energy Agency, the U.S.-EU Task Force on European Energy Security, the Clean Energy Ministerial and Mission Innovation, Power Africa, the Eastern Mediterranean Gas Forum, the Partnership for Transatlantic Energy and Climate Cooperation, and other critical fora, we will drive concrete action to achieve an energy secure future

Reference 10 - 0.05% Coverage

Going forward, the United States must continue to address both acute needs and work collaboratively to build sustained food security for the long term.

Reference 11 - 0.09% Coverage

Nuclear, chemical, and biological weapons proliferation is a vitally important and enduring global challenge, requiring sustained collaboration to prevent the spread of weapons of mass destruction and fissile material, their means of delivery, and enabling technologies.

Reference 12 - 0.04% Coverage

We will continue to lead the world in coordinated efforts to lock down nuclear and radiological materials and prevent terrorist acquisition.

Reference 13 - 0.07% Coverage

We are working with like-minded governments, civil society, and the technology sector to address terrorist and violent extremist content online, including through innovative research collaborations.

Reference 14 - 0.08% Coverage

We will accelerate our efforts to curb the threat posed by transnational organized crime, integrating the vital work of law enforcement with diplomatic, financial, intelligence, and other tools, and in coordination with foreign partners.

Reference 15 - 0.09% Coverage

By doing so in close coordination with our allies and partners, we will establish fair rules while also sustaining our economic and technological edge and shape a future defined by fair competition—because when American workers and companies compete on a level playing field, they win.

Reference 16 - 0.16% Coverage

That includes work through the U.S.-EU Trade and Technology Council to foster transatlantic coordination on semiconductor and critical mineral supply chains, trustworthy artificial intelligence, disinformation, the misuse of technology threatening security and human rights, export controls, and investment screening, as well as through the Indo-Pacific Quad on critical and emerging technologies, open, next-generation digital infrastructure, and people-topeople exchanges.

Reference 17 - 0.07% Coverage

We will advance these efforts through regular interactions, multilateral and institutional collaboration, and regional initiatives, and by implementing the commitments made at the Ninth Summit of the Americas.

Reference 18 - 0.06% Coverage

We will pursue these collaborative efforts while ensuring a fundamentally fair, orderly, and humane approach to migration management that bolster border security and protects our nation.

Reference 19 - 0.07% Coverage

The United States derives security and economic benefits from the region’s democratic stability and institutions, as our shared values provide a basis for collaboration and peaceful dispute resolution.

Reference 20 - 0.08% Coverage

These threats impact security throughout the Americas, including here at home, and we will therefore promote collaboration to help assist civilian police and, strengthen justice systems in the Americas, and expand information sharing with our partners.

Reference 21 - 0.11% Coverage

We have an overriding strategic interest in pursuing and strengthening collaboration through intensified diplomatic engagement with hemispheric partners and institutions based on the premise that advance a vision of a region that is secure, middle class, and democratic is fundamentally in the national security interest of the United States.

Reference 22 - 0.06% Coverage

In coordination with international partners and regional bodies, we will counter democratic backsliding by imposing costs for coups and pressing for progress on civilian transitions.

Reference 23 - 0.05% Coverage

We must build resilience to and mitigate climate change in the region, including through agreements to reduce emissions and more cross-Arctic research collaboration.

Reference 24 - 0.07% Coverage

Across these efforts, we will uphold our commitment to honor Tribal sovereignty and self-governance through regular, meaningful, and robust consultation and collaboration with Alaska Native communities.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 DoD Cyber Strategy Summary - § 8 references coded [ 1.93% Coverage]

Reference 1 - 0.19% Coverage

It has also helped to ensure the superiority of the Joint Force, strengthening our ability to coordinate and quickly adapt to dynamic circumstances.

Reference 2 - 0.34% Coverage

Our global Allies and partners are foundational to the 2023 DoD Cyber Strategy. The United States’ diplomatic and defense relationships represent a force multiplier that extends into cyberspace, enabling rapid coordination and awareness of emerging threats.

Reference 3 - 0.23% Coverage

We will continue hunt forward operations and other bilateral technical collaboration, working with Allies and partners to illuminate malicious cyber activity on their networks.

Reference 4 - 0.25% Coverage

These operations will be primarily conducted by USCYBERCOM, leveraging its authorities and in close coordination with other departments and agencies as well as our global Allies and partners.

Reference 5 - 0.19% Coverage

We will continue to improve and expand coordination across the Federal Government and clearly communicate our priorities to interagency partners.

Reference 6 - 0.39% Coverage

Through both DoD’s security cooperation authorities and collaboration with other Federal departments and agencies that can provide opportunities to engage private sector partners, we will respond to requests from global Allies and partners seeking cybersecurity assistance from U.S. experts.

Reference 7 - 0.10% Coverage

Continue Hunt Forward Operations and Bilateral Technical Collaboration

Reference 8 - 0.24% Coverage

We will stand ready to expose and contest behavior inconsistent with such norms and international law, coordinating across the U.S. Government and with our global Allies and partners.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 National Cybersecurity Strategy - § 73 references coded [ 8.34% Coverage]

Reference 1 - 0.10% Coverage

We are laying the foundations for real-time global collaboration leveraging vast amounts of data and computing power that will unlock scientific discoveries and other public goods of which we cannot yet conceive.

Reference 2 - 0.05% Coverage

We have learned hard lessons and made significant progress in the collaborative defense of our digital ecosystem.

Reference 3 - 0.09% Coverage

Deep and enduring collaboration between stakeholders across our digital ecosystem will be the foundation upon which we make it more inherently defensible, resilient, and aligned with U.S. values.

Reference 4 - 0.15% Coverage

This strategy seeks to build and enhance collaboration around five pillars: (1) Defend Critical Infrastructure, (2) Disrupt and Dismantle Threat Actors, (3) Shape Market Forces to Drive Security and Resilience, (4) Invest in a Resilient Future, and (5) Forge International Partnerships to Pursue Shared Goals.

Reference 5 - 0.10% Coverage

Each effort requires unprecedented levels of collaboration across its respective stakeholder communities, including the public sector, private industry, civil society, and international allies and partners.

Reference 6 - 0.11% Coverage

Together, industry and government must drive effective and equitable collaboration to correct market failures, minimize the harms from cyber incidents to society’s most vulnerable, and defend our shared digital ecosystem.

Reference 7 - 0.09% Coverage

This strategy outlines how the Federal Government will use all tools available to reshape incentives and achieve unity of effort in a collaborative, equitable, and mutually beneficial manner.

Reference 8 - 0.16% Coverage

We must ensure that market forces and public programs alike reward security and resilience, build a robust and diverse cyber workforce, embrace security and resilience by design, strategically coordinate research and development investments in cybersecurity, and promote the collaborative stewardship of our digital ecosystem.

Reference 9 - 0.07% Coverage

It replaces the 2018 National Cyber Strategy but continues momentum on many of its priorities, including the collaborative defense of the digital ecosystem.

Reference 10 - 0.11% Coverage

We aim to operationalize an enduring and effective model of collaborative defense that equitably distributes risk and responsibility, and delivers a foundational level of security and resilience for our digital ecosystem.

Reference 11 - 0.10% Coverage

Collaboration to address advanced threats will only be effective if owners and operators of critical infrastructure have cybersecurity protections in place to make it harder for adversaries to disrupt them.

Reference 12 - 0.14% Coverage

This Administration has conducted sector-specific engagement with industry to construct consistent, predictable regulatory frameworks for cybersecurity that focus on achieving security outcomes and enabling continuity of operations and functions, while promoting collaboration and innovation.

Reference 13 - 0.05% Coverage

Private sector entities have made significant commitments to engage in collaborative defense efforts.

Reference 14 - 0.13% Coverage

The “Shields Up” campaign preceding Russia’s 2022 brutal and unprovoked war on Ukraine, to proactively increase preparedness and promote effective measures to combat malicious activity, is an example of public-private collaboration that must be scaled and repeated.

Reference 15 - 0.12% Coverage

We must build new and innovative capabilities that allow owners and operators of critical infrastructure, Federal agencies, product vendors and service providers, and other stakeholders to effectively collaborate with each other at speed and scale.

Reference 16 - 0.08% Coverage

Federal agencies that support critical infrastructure providers must enhance their own capabilities and their ability to collaborate with other Federal entities.

Reference 17 - 0.08% Coverage

When incidents occur, Federal response efforts must be coordinated and tightly integrated with private sector and State, local, Tribal, and territorial (SLTT) partners.

Reference 18 - 0.13% Coverage

Our strategic environment requires modern and nimble regulatory frameworks for cybersecurity tailored for each sector’s risk profile, harmonized to reduce duplication, complementary to public-private collaboration, and cognizant of the cost of implementation.

Reference 19 - 0.10% Coverage

A collaborative process between industry and regulators will produce regulatory requirements that are operationally and commercially viable and will ensure the safe and resilient operation of critical infrastructure.

Reference 20 - 0.10% Coverage

Where states or independent regulators have authorities that can be used to set cybersecurity requirements, the Administration will encourage them to use those authorities in a deliberate and coordinated manner.

Reference 21 - 0.07% Coverage

ONCD, in coordination with the Office of Management and Budget (OMB), will lead the Administration’s efforts on cybersecurity regulatory harmonization.

Reference 22 - 0.06% Coverage

The Cyber Incident Reporting Council will coordinate, deconflict, and harmonize Federal incident reporting requirements.

Reference 23 - 0.24% Coverage

STRATEGIC OBJECTIVE 1.2: SCALE PUBLIC-PRIVATE COLLABORATION   
Defending critical infrastructure against adversarial activity and other threats requires a model of cyber defense that emulates the distributed structure of the Internet. We will realize this distributed, networked model by developing and strengthening collaboration between defenders through structured roles and responsibilities and increased connectivity enabled by the automated exchange of data, information, and knowledge.

Reference 24 - 0.13% Coverage

Combining organizational collaboration and technologyenabled connectivity will create a trust-based “network of networks” that builds situational awareness and drives collective and synchronized action among the cyber defenders that protect our critical infrastructure.

Reference 25 - 0.04% Coverage

CISA is the national coordinator for critical infrastructure security and resilience.

Reference 26 - 0.10% Coverage

In this role, CISA coordinates with Sector Risk Management Agencies (SRMAs) to enable the Federal Government to scale its coordination with critical infrastructure owners and operators across the United States.

Reference 27 - 0.13% Coverage

The Federal Government will continue to enhance coordination between CISA and other SRMAs, invest in the development of SRMA capabilities, and otherwise enable SRMAs to proactively respond to the needs of critical infrastructure owners and operators in their sectors.

Reference 28 - 0.06% Coverage

The Federal Government will collaborate with industry to define sector-by-sector needs and assess gaps in current SRMA capabilities.

Reference 29 - 0.13% Coverage

SRMAs must also continue to support the maturation of third-party collaboration mechanisms. Building on decades of experience collaborating with ISACs and ISAOs, the Federal Government will work with these and other groups to develop a shared vision of how this model should evolve.

Reference 30 - 0.07% Coverage

Accelerating operational collaboration will require the use of technology solutions to share information and coordinate defensive efforts.

Reference 31 - 0.06% Coverage

We must complement human-to-human collaboration efforts with machine-to-machine data sharing and security orchestration.

Reference 32 - 0.11% Coverage

The Federal Government will also deepen operational and strategic collaboration with software, hardware, and managed service providers with the capability to reshape the cyber landscape in favor of greater security and resilience.

Reference 33 - 0.09% Coverage

The Federal Government must coordinate the authorities and capabilities of the departments and agencies that are collectively responsible for supporting the defense of critical infrastructure.

Reference 34 - 0.11% Coverage

Federal Cybersecurity Centers serve as collaborative nodes that fuse together whole-of-government capabilities across the homeland defense, law enforcement, intelligence, diplomatic, economic, and military missions.

Reference 35 - 0.08% Coverage

Once fully integrated, they will drive intragovernmental coordination and enable the Federal Government to effectively and decisively support non-Federal partners.

Reference 36 - 0.07% Coverage

revitalizing the Cyber Threat Intelligence Integration Center’s (CTIIC) role in coordinating intelligence collection, analysis, and partnerships.

Reference 37 - 0.21% Coverage

Operational collaboration models at SRMAs, such as the Department of Energy (DOE)’s Energy Threat Analysis Center (ETAC) pilot, DoD’s Defense Industrial Base Collaborative Information Sharing Environment (DCISE), and the National Security Agency (NSA)’s Cybersecurity Collaboration Center provide opportunities to enable timely, actionable, and relevant information sharing directly with private sector partners in their respective sectors.

Reference 38 - 0.10% Coverage

ONCD will lead the Administration’s efforts to enhance the integration of centers such as these, identify gaps in capabilities, and develop an implementation plan to enable collaboration at speed and scale.

Reference 39 - 0.11% Coverage

The private sector is capable of mitigating most cyber incidents without direct Federal assistance. When Federal assistance is required, the Federal Government must present a unified, coordinated, whole-of-government response.

Reference 40 - 0.27% Coverage

Consistent with Presidential Policy Directive 41, “United States Cyber Incident Coordination,”— which defines lead roles for the Department of Justice (DOJ), Department of Homeland Security (DHS), and the Office of the Director of National Intelligence in threat, asset, and intelligence   
11 NAT I ONAL CY B E RS E CU RI T Y S T RATEGY   
        
response efforts, respectively—CISA will lead a process to update the subordinate National Cyber Incident Response Plan (NCIRP) to strengthen processes, procedures, and systems to more fully realize the policy that “a call to one is a call to all.”

Reference 41 - 0.09% Coverage

Because most Federal responses take place through field offices, the NCIRP will bolster coordination at the local level, taking lessons from the successes of the Joint Terrorism Task Forces.

Reference 42 - 0.10% Coverage

The Director of the NSA, as the National Manager for NSS, will coordinate with OMB to develop a plan for NSS at FCEB agencies that ensures implementation of the enhanced cybersecurity requirements of NSM-8.

Reference 43 - 0.09% Coverage

Coordinated efforts by Federal and non-Federal entities have proven effective in frustrating the malicious cyber activity of foreign government, criminal, and other threat actors.

Reference 44 - 0.12% Coverage

Our efforts will require greater collaboration by public and private sector partners to improve intelligence sharing, execute disruption campaigns at scale, deny adversaries use of U.S.-based infrastructure, and thwart global ransomware campaigns.

Reference 45 - 0.20% Coverage

DoD’s new strategy will clarify how U.S. Cyber Command and other DoD components will integrate cyberspace operations into their efforts to defend against state and non-state actors capable of posing strategic-level threats to U.S. interests, while continuing to strengthen their integration and coordination of operations with civilian, law enforcement, and intelligence partners to disrupt malicious activity at scale.

Reference 46 - 0.10% Coverage

The NCIJTF, as a multi-agency focal point for coordinating whole-of-government disruption campaigns, will expand its capacity to coordinate takedown and disruption campaigns with greater speed, scale, and frequency.

Reference 47 - 0.11% Coverage

Effective disruption of malicious cyber activity requires more routine collaboration between the private sector entities that have unique insights and capabilities and the Federal agencies that have the means and authorities to act.

Reference 48 - 0.10% Coverage

The 2021 takedown of the Emotet botnet showed the potential of this collaborative approach, with Federal agencies, international allies and partners, and private industry cooperating to disrupt the botnet’s operations.

Reference 49 - 0.13% Coverage

Private sector partners are encouraged to come together and organize their efforts through one or more nonprofit organizations that can serve as hubs for operational collaboration with the Federal Government, such as the National Cyber-Forensics and Training Alliance (NCFTA).

Reference 50 - 0.07% Coverage

The timely sharing of threat intelligence between Federal and non-Federal partners enhances collaborative efforts to disrupt and dismantle adversaries.

Reference 51 - 0.10% Coverage

For instance, the NSA Cybersecurity Collaboration Center’s national intelligence-driven engagement with industry has been highly effective at disrupting adversary activity targeting the Defense Industrial Base.

Reference 52 - 0.09% Coverage

The Administration is committed to mounting disruption campaigns and other efforts that are so sustained, coordinated, and targeted that they render ransomware no longer profitable.

Reference 53 - 0.18% Coverage

The United States subjects financial institutions offering covered services in   
17 NAT I ONAL CY B E RS E CU RI T Y S T RATEGY   
        
cryptocurrencies to Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) controls, and the Department of the Treasury, the Secret Service, DOJ, the FBI, and private sector partners are collaborating to trace and interdict ransomware payments.

Reference 54 - 0.09% Coverage

To further incentivize the adoption of secure software development practices, the Administration will encourage coordinated vulnerability disclosure across all technology types and sectors

Reference 55 - 0.10% Coverage

The Federal Government will collaborate with SLTT entities, the private sector, and other partners to balance cybersecurity requirements for applicants with technical assistance and other forms of support.

Reference 56 - 0.08% Coverage

We can build a more secure, resilient, privacy-preserving, and equitable digital ecosystem through strategic investments and coordinated, collaborative action.

Reference 57 - 0.13% Coverage

The Administration is coordinating the work of stakeholders across the Federal Government, industry, and SLTT to deploy a secure, interoperable network of electric vehicle chargers, zero-emission fueling infrastructure, and zero-emission transit and school buses.

Reference 58 - 0.18% Coverage

To counter common threats, preserve and reinforce global Internet freedom, protect against transnational digital repression, and build toward a shared digital ecosystem that is more inherently resilient and defensible, the United States will work to scale the emerging model of collaboration by national cybersecurity stakeholders to cooperate with the international community.

Reference 59 - 0.22% Coverage

We will expand coalitions, collaboratively disrupt transnational criminals and other malicious cyber actors, build the capacity of our international allies and partners, reinforce the applicability of existing international law to state behavior in cyberspace, uphold globally accepted and voluntary norms of responsible state behavior in peacetime, and punish those that engage in disruptive, destructive, or destabilizing malicious cyber activity.

Reference 60 - 0.14% Coverage

In April 2022, the United States and 60 countries launched the Declaration for the Future of the Internet (DFI), bringing together a broad, diverse coalition of partners—the largest of its kind— around a common, democratic vision for an open, free, global, interoperable, reliable, and secure digital future.

Reference 61 - 0.24% Coverage

The Indo-Pacific Economic Framework for Prosperity (IPEF) and the Americas Partnership for Economic Prosperity (APEP) create opportunities for the United States and regional governments to collaborate in setting rules of the road for the digital economy, including facilitating the development of technical standards, mechanisms to enable cross-border data flows that protect privacy while avoiding strict data localization requirements, and actions to foster supply chain security and resilience.

Reference 62 - 0.11% Coverage

The United States is also working closely with Australia and the United Kingdom through the trilateral security and technology pact (“AUKUS”) to secure critical technologies, improve cyber coordination, and share advanced capabilities.

Reference 63 - 0.17% Coverage

Through these and other partnerships, the United States and international counterparts can advance common cybersecurity interests by sharing cyber threat information, exchanging model cybersecurity practices, comparing sector-specific expertise, driving secure-by-design principles, and coordinating policy and incident response activities.

Reference 64 - 0.06% Coverage

We will leverage these partnerships to enable effective operational collaboration to defend our shared digital ecosystem.

Reference 65 - 0.14% Coverage

Because most malicious cyber activity targeting the United States is carried out by actors based in foreign countries or using foreign computing infrastructure, we must strengthen the mechanisms we have to collaborate with our allies and partners so that no adversary can evade the rule of law.

Reference 66 - 0.06% Coverage

The United States will work with its allies and partners to develop new collaborative law enforcement mechanisms for the digital age.

Reference 67 - 0.21% Coverage

We must enable our allies and partners to secure critical infrastructure networks, build effective incident detection and response capabilities, share cyber threat information, pursue diplomatic collaboration, build law enforcement capacity and effectiveness through operational collaboration, and support our shared interests in cyberspace by adhering to international law and reinforcing norms of responsible state behavior.

Reference 68 - 0.13% Coverage

To accomplish this goal, the United States will marshal expertise across agencies, the public and private sectors, and among advanced regional partners to pursue coordinated and effective international cyber capacity-building and operational collaboration efforts.

Reference 69 - 0.12% Coverage

Increasingly, a community of nations has collaborated to produce coordinated statements of attribution that carry the simultaneous diplomatic condemnation of many governments and strengthening the coalition committed to a stable cyberspace.

Reference 70 - 0.10% Coverage

These efforts will require collaborative use of all tools of statecraft, including diplomatic isolation, economic costs, counter-cyber and law enforcement operations, or legal sanctions, among others.

Reference 71 - 0.11% Coverage

Mitigating this risk will require long-term, strategic collaboration between public and private sectors at home and abroad to rebalance global supply chains and make them more transparent, secure, resilient, and trustworthy.

Reference 72 - 0.10% Coverage

Critical inputs, components, and systems must increasingly be developed at home or in close coordination with allies and partners who share our vision of an open, free, global, interoperable, reliable, and secure Internet.

Reference 73 - 0.12% Coverage

Extending this model to other critical technologies will require long-term, strategic collaboration between public and private sectors at home and abroad to rebalance global supply chains and make them more secure, resilient, and trustworthy.