AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Calendar No. 698

111TH CONGRESS *2d Session*	SENATE	REPORT 111–368

PROTECTING CYBERSPACE AS A NATIONAL ASSET ACT OF 2010

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 3480

TO AMEND THE HOMELAND SECURITY ACT OF 2002 AND OTHER LAWS TO ENHANCE THE SECURITY AND RESILIENCY OF THE CYBER AND COMMUNICATIONS INFRASTRUCTURE OF THE UNITED STATES

DECEMBER 15, 2010.—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE

99–010 WASHINGTON : 2010

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan	SUSAN M. COLLINS, Maine
DANIEL K. AKAKA, Hawaii	TOM COBURN, Oklahoma
THOMAS R. CARPER, Delaware	SCOTT P. BROWN, Massachusetts
MARK L. PRYOR, Arkansas	JOHN MCCAIN, Arizona
MARY L. LANDRIEU, Louisiana	GEORGE V. VOINOVICH, Ohio
CLAIRE MCCASKILL, Missouri	JOHN ENSIGN, Nevada
JON TESTER, Montana	LINDSEY GRAHAM, South Carolina
CHRISTOPHER A. COONS, Delaware	MARK KIRK, Illinois

MICHAEL L. ALEXANDER, *Staff Director*
KEVIN J. LANDY, *Chief Counsel*
DEBORAH P. PARKINSON, *Professional Staff Member*
ADAM R. SEDGEWICK, *Professional Staff Member*
JEFFREY E. GREENE, *Counsel*
JEANETTE HANNA-RUIZ, *DHS Detailee*
BRANDON L. MILHORN, *Minority Staff Director and Chief Counsel*
ROBERT L. STRAYER, *Minority Director for Homeland Security Affairs*
ASHA A. MATHEW, *Minority Senior Counsel*
JOHN K. GRANT, *Minority Counsel*
DEVIN F. O'BRIEN, *Minority Professional Staff Member*
DENISE E. ZHENG, *Minority Professional Staff Member*
TRINA DRIESSNACK TYRER, *Chief Clerk*

Calendar No. 698

111TH CONGRESS, 2d Session | SENATE | REPORT 111–368

PROTECTING CYBERSPACE AS A NATIONAL ASSET ACT OF 2010

DECEMBER 15, 2010.—Ordered to be printed

Mr. LIEBERMAN, from the Committee on Homeland Security and Governmental Affairs, submitted the following

R E P O R T

[To accompany S. 3480]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 3480) to amend the Homeland Security Act of 2002 and other laws to enhance the security and resiliency of the cyber and communications infrastructure of the United States, having considered the same, reports favorably thereon with an amendment and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

S. 3480, the Protecting Cyberspace as a National Asset Act of 2010, seeks to modernize and strengthen the federal government's ability to safeguard the nation from cyber attacks. It would do so by creating a National Center for Cybersecurity and Communications (NCCC) within the Department of Homeland Security (DHS) that would be responsible for protecting both federal computer networks and critical infrastructure owned by the private sector against cyber attacks. The bill would also bring greater unity and efficiency to federal cybersecurity efforts by establishing a White

House Office of Cyberspace Policy to coordinate federal work in the area and to advise the President on cybersecurity issues.

II. Background and Need for the Legislation

Threats to information systems and assets

The history of the Internet begins with a Department of Defense project that sought to maintain command and control over its missiles and bombers after a nuclear attack—a system that would allow communication to continue working even if one node was attacked. In 1969, the project created ARPANET, a computer link between UCLA and Stanford which allowed academics and members of the research community to send packets of digital information to each other over computer networks. Ironically, this system which was conceived of to ensure communication during a national security crisis was itself never designed to be secure.

Over the next 20 years, it remained a system used primarily by researchers and scientists in academia and government—a community where trust was not an issue and openness and easy access were seen as necessary for innovation. In the 1990s, the Internet was made available to a variety of commercial and governmental uses and the personal computer became more powerful and affordable. Today, the Internet permeates our society—it is an essential element for communication and for operating our financial systems, transportation systems, shipping, electrical power grid, oil and gas pipelines, nuclear plants, water systems, manufacturing, and the military. As of this year, over 1.9 billion people use the Internet, and more come online every day.[1]

Unfortunately, increased security has not fully accompanied this exponential growth. The combination of increasingly valuable information stored and accessible online and the growing use of the Internet to control components of our most critical infrastructure, coupled with the explosion of entry points and potential victims, has made the Internet an attractive avenue for new breeds of criminals, spies and warriors to exploit. They look at the Internet and see a gateway to everything from our personal bank accounts to industrial and government secrets to the very infrastructure—the electric, utilities and financial sectors—our economy needs to function.

Economic consequences

Security experts estimate that $1 trillion a year is lost to cybercrime.[2] The computer security company McAfee surveyed executives of companies involved in critical infrastructure and reported that 54 percent said their companies had been the victims of denial of service attacks as well as network infiltration from organized crime groups, terrorists, and other nation-states. The downtime to recover from these attacks can cost as much as $6 million to $8 million a day.[3]

---

[1] *The World In 2009: Facts and Figures,* International Trade Union, http://www.itu.int/ITU-D/ict/material/Telecom09_flyer.pdf.

[2] McAfee Report, "In the Crossfire: Critical Infrastructure in the Age of Cyber-War," January 2010.

[3] Ibid.

In December 2009, Google and 30 other companies in the information technology, finance, technology, media and chemical sectors—most of them global Fortune 500 companies—were the targets of highly sophisticated attacks allegedly emanating from China in what appears to have been a massive attempt at industrial espionage and theft of intellectual property.[4]

In 2007, TJX Corporation—the parent company of T.J. Maxx and Marshall's department stores—experienced a breach in its wireless networks that left about 45 million credit and debit card numbers exposed to theft and cost the company about $25 million to resolve.[5] In early 2009, Heartland Payment Systems learned they had suffered a breach that allowed criminal access to in-transit payment card data, requiring them to spend $32 million in the first half of 2009 to resolve. Later, Albert Gonzales was indicted for both the TJX and Heartland attacks, among others.[6]

It is not just large corporations that are vulnerable. Cyber criminals have stolen millions of dollars from small- to medium-sized businesses and local governments. In one incident, for example, unsuspecting financial officers received a seemingly innocuous e-mail that contained either a virus or an Internet link that installed a tiny piece of malicious computer code designed to steal passwords. The crooks would then patiently steal amounts less than the $10,000 that otherwise would have triggered a bank report under federal anti-money laundering requirements. The malicious code was so well written that the traffic seemed to be coming from an authorized computer and the bank could not see anything amiss. As a result of this scam, a school district near Pittsburgh lost $700,000; an electronics testing firm in Baton Rouge had $100,000 disappear from its bank account, and a Texas manufacturing firm found itself short $1.2 million.[7]

The Committee learned, during publicly held hearings, that the profits from some of these Internet fraud schemes are used to funnel money to terrorist organizations, which then use the funds to finance attacks against the United States and its allies.[8]

NATIONAL SECURITY

Beyond the commercial and industrial threats posed by this new breed of cyber criminal, the United States also must be prepared for the very real possibility of "cyber-war," "cyber espionage," or "cyber-terrorism." We have known about these threats for years, and recently received confirmation that other countries will not shy away from opening a new front in cyberspace.

Indeed, the concept of "cyber war" has required us to rethink the very notion of war itself, because threats to U.S. national security reach beyond military targets to critical infrastructure and the economy. In 2009, the Wall Street Journal reported that hackers have penetrated the U.S. electrical grid, mapped out the infrastruc-

---

[4] The Official Google Blog, "A New Approach to China," Jan. 12, 2010, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

[5] The Boston Globe, TJX Cost for Breach at $25 Million So Far, May 16, 2007.

[6] *See* Statement of Robert Carr, Chairman and CEO, Heartland Payment Systems, for hearing entitled, "Cyber Attacks: Protecting Industry Against Growing Threats" U.S. Senate Committee on Homeland Security and Governmental Affairs, September 14, 2009 at 2–3.

[7] The Washington Post, "European Gangs Target Small U.S. Firms," Aug. 25, 2009.

[8] *See* Statement of Tom Kellerman, Vice President of Security Awareness, Core Security Technologies, for hearing entitled, "Cyber Security: Developing a National Strategy" U.S. Senate Committee on Homeland Security and Governmental Affairs, April 28th, 2009 at 2.

ture, and left behind software programs that could be used to disrupt systems operating the grid.[9] That same year, CIA analyst Tom Donahue, speaking before a power industry conference, warned that "we have information from multiple regions outside the United States, of cyber-intrusion into utilities followed by extortion demands."[10]

The possibility of attacks on civilian or non-military infrastructure as an adjunct to an armed conflict is real. The Russian invasion of Georgia in August 2008, for example, was accompanied by cyber attacks that took down Georgian government websites and denied Georgian civilians access to news and other online computer services.[11]

And the threat of a major and intentional cyber disruption can arise entirely outside the context of conventional warfare. In 2000, an Australian engineer angry at his former employer and a city government that refused to give him a job used his computer expertise to order local sewer systems to dump 200,000 gallons of raw sewage into local parks and rivers, killing marine life and turning a local creek black with an unbearable stench.[12]

These kinds of attacks and intrusions are becoming pervasive, reported the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency. According to the Commission's 2008 report, the Departments of Defense, State, Homeland Security and Commerce, as well as NASA and the National Defense University, have all suffered "major intrusions by unknown foreign entities"—and Department of Defense computers are being probed hundreds of thousands of times a day.[13]

Some of the more troubling security breaches that have been reported in recent years include:

- The Commerce Department was forced to take down for months the computer systems of the Bureau of Industry and Security, whose mission is to "advance national security, foreign policy, and economic objectives by ensuring an effective export control and treaty compliance system and promoting continued U.S. strategic technology leadership."[14]
- NASA's designs for new rocket launchers appear to have been compromised.[15]
- The State Department lost "terabytes" of information.[16]
- The unclassified e-mail of the Secretary of Defense was hacked.[17]

---

[9] Wall Street Journal, "Electricity Grid in U.S. Penetrated By Spies," April 8, 2009, http://online.wsj.com/article/SB123914805204099085.html

[10] Reuters, "Has Power Grid Been Hacked? U.S. Won't Say," April 8, 2009, http://www.reuters.com/article/idUSN0850385920090408.

[11] The New York Times, "U.S. Steps up Efforts on Digital Defenses," April 27, 2009, http://www.nytimes.com/2009/04/28/us/28cyber.html.

[12] National Institute of Standards and Technology, Computer Security Resource Center, Malicious Control System Cyber Security Attack Case Study—Maroochy Water Services, Australia, http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf.

[13] Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency, "Securing Cyberspace for the 44th Presidency", at http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

[14] Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency, "Threats Posed to the Internet", at http://csis.org/files/media/csis/pubs/081028_threats_working_group.pdf.

[15] Ibid.

[16] Ibid.

[17] Ibid.

• A foreign intelligence agency inserted malicious code onto U.S. Central Command's classified military computer networks.[18]

• Stuxnet, a computer worm that was designed specifically to infiltrate industrial control systems and had the potential overwrite commands to sabotage industrial facilities, was found on computer systems around the world.

Besides exposing national security secrets that could give our opponents advance warning of our tactics, strategies and capabilities, this kind of espionage can lead to a loss of valuable military technologies and intellectual property that can cost the United States billions of dollars to develop and result in even more billions lost in economic benefits from innovation. "We are not arming our competitors in cyberspace; we are providing them with the ideas and designs to arm themselves and achieve parity," the CSIS report said.[19]

Countries like China are actively building up cyber capabilities as part of their national security strategy. According to a Nov. 7, 2007 report by the bipartisan, congressionally-chartered U.S.-China Economic and Security Review Commission: "Chinese espionage in the United States, now comprises the single greatest threat to the U.S. . . . Chinese military strategists have embraced disruptive warfare techniques, including the use of cyber attacks, and incorporated them in China's military doctrine. Such attacks, if carried out strategically on a large scale, could have catastrophic effects on the target country's critical infrastructure." [20]

WHITE HOUSE OFFICE OF CYBERSPACE POLICY

The CSIS cybersecurity report found that: "Our government is still organized for the Industrial Age, for assembly lines and mass production. It is a giant, hierarchal conglomerate where the cost of obtaining information and making decisions is high when this requires moving across organizational boundaries." This kind of organization does not work in the age of the Internet and has helped create the kinds of Internet vulnerabilities we are experiencing now, the report said.

CSIS recommended the creation of an office within the White House, headed by a Senate-confirmed Director who would oversee the broad contours of a new cybersecurity strategy, advise the President, and work with other executive branch agencies to implement the strategy and resolve any disputes.

The Obama Administration, which conducted its own "Cyberspace Policy Review" at the beginning of 2009, came to a similar conclusion:

> *It's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation. It's also clear that we're not as prepared as we should be, as a government or as a country. . . . No single official oversees cybersecurity policy across the federal government, and no single agency has the responsibility or authority to*

[18] Lynn, W.. (2010). Defending a New Domain. Foreign Affairs, 89(5), 97–108. Retrieved December 10, 2010, from ABI/INFORM Global. (Document ID: 2129061161).

[19] Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency, "Securing Cyberspace for the 44th Presidency", at 13.

[20] U.S.-China Economic and Security Review Commission, 2007 Report to Congress, November 2007, p. 7, www.uscc.gov/annual_report/2007/07_annual_report.php.

match the scope and scale of the challenge. Indeed, when it comes to cybersecurity, federal agencies have overlapping missions and don't coordinate and communicate nearly as well as they should—with each other or with the private sector.[21]

The President established a small Cybersecurity Directorate within the National Security Staff and tasked it with coordinating cyber security activities across the federal government. The head of the Directorate reports to both the National Security Council and National Economic Council leadership.

The Committee agrees with the CSIS report and the President that White House leadership is needed to ensure a coordinated federal cybersecurity effort. The Committee believes, however, that establishing leadership within the NSC structure does not go far enough. S. 3480 instead would establish an Office of Cyberspace Policy within the Executive Office of the President to oversee all aspects of cyberspace policy, including military, law enforcement, intelligence, and diplomatic. A Senate-confirmed Director, accountable to the American people and to Congress, would lead the office.

The Director of Cyberspace Policy would perform all the duties the President envisioned for the current Cybersecurity Directorate, with some important additions. The new office would also review budget requests relating to the national cybersecurity strategy and settle inter-agency disputes relating to the strategy and matters of policy.

DHS ROLE AND ORGANIZATION

While the new Office of Cyberspace Policy would help lead and harmonize the Federal government's efforts, the Committee believes that more needs to be done on an operational level to protect government systems and critical infrastructure. To accomplish this, S. 3480 would create a new operational entity within DHS: the National Center for Cybersecurity and Communications (NCCC). The NCCC would sharpen our nation's focus on the security of civilian government systems and private sector networks, especially those that are most critical to our nation's welfare. The NCCC would partner with the private sector, in an effort to better understand and address the risks our nation faces from cyber threats.

DHS already has the responsibility to protect the nation's federal civilian networks and to coordinate federal efforts to secure the nation's most critical infrastructure, including its cyber infrastructure. S. 3480 codifies these existing responsibilities and provides additional resources and tools necessary to ensure that DHS will succeed in this crucial mission.

Title II of the Homeland Security Act of 2002, which created DHS, directs the Department to lead critical infrastructure protection efforts. Critical infrastructure is defined in the Act as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating effect on security, national economic security, national public health or safety, or any combination of these matters."[22] The Internet is itself critical infrastructure, and

[21] http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.
[22] P.L. 107–296 (citing P.L. 107–56).

is increasingly essential to the reliable operation of many other critical infrastructure sectors. It is one of the main drivers of our economy, and is increasingly a key component of our national defense systems.

A year after the Homeland Security Act was passed, President Bush released the National Strategy to Secure Cyberspace, which stated that DHS would be the "focal point for the federal government to manage cybersecurity."[23] Later in 2003, the White House issued Homeland Security Presidential Directive 7 (HSPD–7) to implement the critical infrastructure responsibilities laid out in the Homeland Security Act. HSPD–7 reinforced the leadership role of DHS on cybersecurity, stating, "the Secretary of Homeland Security will continue to maintain an organization to serve as a focal point for the security of cyberspace."[24]

In 2008, President Bush issued Homeland Security Presidential Directive 23 (HSPD–23) to implement the Comprehensive National Cybersecurity Initiative, which mainly focused on the protection of government networks. In HSPD–23, the President affirmed that DHS serves as the lead federal agency for the protection of all unclassified federal networks and for coordinating private sector cybersecurity efforts.

Despite considerable progress, the Committee believes that the Department needs additional authorities to be successful in these missions. This includes additional authorities that previously belonged to the Office of Management and Budget relating to federal information security and the authority to set risk-based security performance requirements for our nation's most critical cyber infrastructure.

The NCCC would be led by a Senate-confirmed Director, who would regularly advise the President regarding the exercise of authorities relating to the security of federal networks. The NCCC would include the United States Computer Emergency Response Team (US–CERT), and it would lead federal operational efforts to protect public and private sector networks. The NCCC would detect, prevent, analyze, and warn of cyber threats to these networks.

Specifically, the NCCC would produce and share warning, analysis, and threat information with the private sector, other federal agencies, state and local governments, and international partners. It would also collaborate with the private sector to develop and promote best practices to help improve cybersecurity across the nation. The Center would provide technical assistance to private sector entities and state and local governments, as requested and permitted by resources, to help implement best practices, assess vulnerabilities, or otherwise improve the security of cyber networks. Sensitive information shared by the private sector with the NCCC, such as notifications of vulnerabilities or security breaches, would be protected from public disclosure. The bill encourages the NCCC to ensure that private sector owners and operators are able to obtain security clearances to access threat analysis and other information necessary to protect critical systems and assets.

The Committee believes that by working in partnership and voluntarily sharing information with the private sector, the NCCC

---

[23] "*The National Strategy to Secure Cyberspace*" February 2003, pg. 22.

[24] "*Homeland Security Presidential Directive—7, Critical Infrastructure Identification, Prioritization, and Protection.*" December 17, 2003.

would have a better understanding of the threats and vulnerabilities our nation faces in cyberspace and would gain true "situational awareness" of the nation's overall cybersecurity posture.

This situational awareness would be developed with strong privacy and civil liberty protections incorporated from the beginning. The bill would require the Director of the NCCC to develop specific guidelines to protect the privacy and civil liberties of U.S. Persons, which would be done in conjunction with the privacy officer of the NCCC. The Fair Information Practices developed by DHS should serve as the starting point for these guidelines. The bill creates no new authority to conduct electronic surveillance or to compel the disclosure of private information.

CRITICAL INFRASTRUCTURE

Today the Internet impacts our lives in ways that most of us never see or even think about. It is no longer simply a mechanism for communication. Indeed, it plays an increasingly essential role in the things that make our very way of life possible, from the electricity that powers our homes, to the water we drink, to the gasoline we put in our cars. However, while the use of the Internet has brought increased efficiency to our industry and infrastructure, it has also brought with it increased risks. A system that is controlled over the Internet by its rightful owners is also a system that can be penetrated and potentially "owned" by a criminal, a spy, an enemy nation, or a terrorist.

In 2007, the Department of Homeland Security demonstrated how vulnerable the country's most critical infrastructure is to a cyber attack. Many industrial processes are now automated and controlled by Supervisory Control and Data Acquisition systems (or SCADA systems). SCADA systems help to generate electricity, control the amount of water flowing through a dam, and operate nuclear power plants. In recent years, companies have increased efficiency and reduced cost by controlling SCADA systems over the Internet. For example, an electric facility no longer needs to send a technician to operate a remote substation in person when it can be done through a keyboard located in their headquarters for a fraction of the cost. However, this convenience comes with a security price. In an experiment named "Aurora," DHS demonstrated that an electrical generator connected to the Internet could be accessed remotely and given instructions that would literally cause it to self-destruct. A skilled enemy exploiting such a vulnerability on a mass scale could plunge our cities into darkness for weeks or months. Perhaps even more disturbing, this same risk is present in many other critical infrastructure sectors, such as nuclear power plants and water treatment facilities.

The emergence of the "Stuxnet" worm in the summer of 2010 demonstrated that a cyber attack on SCADA systems is no longer just a theoretical concern. According to numerous experts, Stuxnet was designed to target critical infrastructure control systems. While other worms have impacted these systems, Stuxnet is the first that actually seeks them out. Moreover, forensic analyses conducted by private sector experts have concluded that this worm is designed not just to steal information, but to take control of the mechanical processes of physical machinery. Thus, the machinery can be made to do whatever Stuxnet's authors want it to do, irre-

spective of the commands being given by the operators. Stuxnet has been found on systems around the world, including systems in the United States.

The federal government must ensure that SCADA systems controlling our most critical infrastructure are not just minimally protected, but that they all maintain a high level of security consistent with the risk that a disruption could cause catastrophic damage. To achieve the security we need, S. 3480 would establish a collaborative, cooperative partnership between our most critical infrastructure providers and our government.

The bill would direct the NCCC to work with the private sector to develop risk-based security performance requirements to strengthen the cybersecurity of the nation's most critical infrastructure, including vital components of the electric grid, telecommunications networks, and control systems in other critical infrastructure that, if disrupted, would result in a national or regional catastrophe. Owners and operators of covered critical infrastructure would choose which security measures to implement to meet these risk-based security performance requirements. The NCCC would review and approve the measures selected, but could not approve or disapprove the proposed security plan based on the presence or absence of a particular security measure.

Covered critical infrastructure would also have to report significant breaches to the NCCC to ensure the federal government has insight into the cyber risks that affect these crucial systems. The NCCC, in turn, would have to share information, including threat analyses, with owners and operators regarding risks to their networks. The Act would also provide protection against punitive and some non-economic damages to owners and operators of covered critical infrastructure who submit to DHS evaluations, successfully demonstrate compliance with their approved security plan during the evaluation, and can prove actual compliance at the time of any breach. This protection would only apply to harm directly caused by the breach, and would not affect any other types of damages sought as a result of it. Additionally, these provisions would not protect an owner or operator from any intervening act, omission, or negligence, even if the harm caused could also be attributed in some way to the breach.

As noted, only those systems or assets whose disruption would cause a national or regional catastrophe would be subject to mandatory risk-based security performance requirements. DHS currently interprets "national or regional catastrophe" to include a combination of the following factors: greater than 2,500 prompt fatalities; greater than $25 billion in first-year economic consequences; mass evacuations with a prolonged absence of greater than one month; or severe degradation of the nation's security capabilities. The Committee expects that the Department would continue to apply a similar standard in implementing S. 3480.

Thus, the bill would establish a process that narrowly defines the systems and assets that the Secretary of Homeland Security could designate as covered critical infrastructure. Additionally, owners and operators who believe that a system or asset was erroneously designated as covered critical infrastructure would have the opportunity to appeal that designation. The NCCC would be required to coordinate with other federal agencies to avoid duplicative regu-

latory requirements and to maximize the efficient use of government resources.

EMERGENCY AUTHORITIES

In February 2010, the Bipartisan Policy Center sponsored an exercise called "Cyber ShockWave," which simulated a massive cyber attack on the United States.[25] During the exercise, former Deputy Attorney General Jamie Gorelick, who played the role of the Attorney General, expressed concern that the President's authorities during a cyber attack are unclear. In particular, she noted on several occasions during the exercise that there is no defined authority or settled law controlling what the President can direct the private sector to do, even if a threat to the private sector could cause mass casualties or catastrophic economic loss.[26]

The Obama Administration echoed this concern in its 2009 "Cyberspace Policy Review," where it noted the continuing ambiguity over "what authorities are available for the government to protect privately owned critical infrastructure." [27]

In testimony before the Committee, DHS Deputy Undersecretary Philip Reitinger asserted that the federal government believes it may have the authority to direct private sector response to a cyber emergency under Section 706 of the Telecommunications Act of 1934 and other unspecified laws.[28] The Committee understands that Section 706 gives the President the authority to take over wire communications in the United States and, if the President so chooses, shut a network down.[29] But it is not clear that the President could order a lesser action, such as the blocking of a particular malicious signature or directing a company outside of the communications sector, such as an electricity generation facility, to take action to protect its cyber networks. It is this gap that S. 3480 is meant to fill.

The bill would establish clear authority for the President, in the event of an actual or imminent attack on covered critical infrastructure, to direct certain limited emergency measures to protect the American people. It would allow the President to take such action quickly, without any debate over what authorities the government actually has or the need to resort to the drastic measure of taking over an entire communications network. Moreover, the bill would require notification to Congress on the threat and proposed response prior to any emergency declaration, unless the nature of the attack required that the notice be provided as soon as possible after a declaration.

S. 3480 would do this by creating a process through which the President could authorize emergency measures, limited in both scope and duration, to protect the nation's most critical infrastructure if a cyber vulnerability was being exploited or was about to

[25] Bipartisan Policy Center is a non-profit organization established to "develop and promote solutions that can attract public support and political momentum in order to achieve real progress." See http://www.bipartisanpolicy.org/about.

[26] http://transcripts.cnn.com/TRANSCRIPTS/1002/20/se.01.html.

[27] White House Cyberspace Policy Review at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf, pg. 3.

[28] *See* Statement of Philip R. Reitinger, Deputy Under Secretary, National Protection and Programs Directorate, U.S. Department of Homeland Security, for hearing entitled, "Protecting Cyberspace as a National Asset: Comprehensive Legislation for the 21st Century" U.S. Senate Committee on Homeland Security and Governmental Affairs, June 15, 2010 at 8.

[29] 47 U.S.C.§606.

be exploited. The bill would require the President to notify Congress of the threat, why existing security practices are inadequate to mitigate the threat, and what emergency measures are necessary to protect the American public. Any emergency measures imposed must be the least disruptive necessary to respond to the threat, and would expire after 30 days unless the President orders an extension. Congress would have to approve any extension of the emergency authorities beyond 120 days.

In determining whether an emergency measure is the "least disruptive means" possible, the bill requires the President to consider not just the impact to the affected system, but also the broader impact the measure would have on the overall national information infrastructure. The bill expressly precludes the President from "taking over" any covered critical infrastructure, and it does not authorize any new surveillance authorities. The President must also ensure that the privacy and civil liberties of the American people are protected while emergency measures are in place.

FISMA REFORM

In the mid-1990's, Congress was concerned that previously isolated, mission critical, federal information systems were becoming increasingly interconnected to an ever-expanding Internet. In 2002, Congress passed the Federal Information Security Management Act (FISMA)[30] to protect sensitive government information and information systems from unauthorized access or destruction by employees, outside hackers, terrorists, or even nation-states. The legislation, at its core, established a risk-based framework whereby the National Institute of Standards and Technology (NIST) developed minimum standards of security protection for agencies based on the criticality of the information and the information system operated by the agency. Agencies were then responsible for implementing the standards developed by NIST to ensure adequate security of their systems and information. The Office of Management and Budget (OMB) coordinated and managed the implementation of FISMA government-wide, requiring agencies to certify and accredit major information systems every 3 years. Inspectors General (IG) then evaluate whether agencies appropriately conducted certifications and accreditations, thereby determining whether agencies adequately managed the risks to their systems. FISMA also established an information security incident response center to help agencies analyze threats to their system.

The Committee believes that FISMA established a foundation for the government to ensure risk-based and cost-effective security but was not implemented in a manner that effectively helped agencies to secure their systems. The Act must be strengthened and streamlined, both legislatively and through more effective Executive Branch implementation. Title III of S. 3480 reflects lessons learned over the past eight years of FISMA implementation, input from leading public and private sector cybersecurity experts, numerous public hearings and closed-door classified briefings, and Committee investigations.

The Committee attributes a large part of FISMA's implementation failures to the limited budget, staff, and technical capability of

[30] P.L. 107–347.

OMB. Although OMB has talented and skilled employees, the Office of Information and Regulatory Affairs and the Office of Electronic Government and Information Technology, the two OMB offices charged with implementing the law, do not have the resources to manage all of the priorities surrounding information policy, of which information security is only a subset. In practice, OMB has effectively relied on agencies to self-police their own decision making and security.

Similarly, while the threat landscape is constantly evolving, the process by which NIST develops information security standards can take years. Agencies testified before the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security that these standards, and NIST guidance in general, do not provide enough operational information on how to best align security controls to the threat landscape.

Without that information, agencies have been left to make independent decisions on how to best secure their systems from all manner of threats. But cybersecurity is typically not a primary mission for many agencies, and most do not have personnel with the security clearances needed to fully understand the evolving threat. As a result, many agencies are left with inadequate protection.

Further, there are no commonly accepted government-wide standards or guidance on how to effectively evaluate agency information security programs to guide IG reviews. Instead, OMB implementation guidance on FISMA is interpreted differently from agency to agency, and agencies often rely on private sector contractors to execute the evaluation instead of the IG. Often agencies overlook key elements of their information infrastructure, including mainframes and messaging services. Additionally, IGs often lack access to classified threat information to evaluate whether agencies are appropriately managing their risks. In short, FISMA has become little more than a paperwork exercise, rather than the dynamic and effective security program it was meant to be.[31]

S. 3480 continues the risk-management framework laid out in 2002, but addresses shortfalls by amending the law in several key areas. Most important, the bill would transfer oversight of cybersecurity within civilian agencies from OMB to the newly established NCCC, which would have significantly more staff, technical capabilities, and resources to both prevent cyber attacks and assist agencies if such attacks do occur. Further, the bill would ensure that agency Chief Information Security Officers (CISO) have access to classified threat information to make the necessary risk-based decisions to defend their networks. The bill also requires agencies to test their security programs through an operational evaluation. These operational evaluations would simulate hackers trying to infiltrate, modify, steal, or destroy agencies' sensitive information and critical systems and would be conducted by teams of individuals who work for either the agency or the NCCC. Lastly, the bill would establish an interagency Federal Information Security

[31] *More Security, Less Waste: What Makes Sense for our Federal Cyber Defense.* Senate Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, October 2009 and *Agencies in Peril: Are We Doing Enough To Protect Federal IT and Secure Sensitive Information?* Senate Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, March 2008.

Taskforce, which would allow the Executive Branch sufficient flexibility to work within the law's framework to handle new and emerging threats.

These changes included in the legislation should improve security while decreasing the cost of FISMA compliance across the government.

FEDERAL PROCUREMENT

Section 253 of the bill requires the DHS Secretary, in collaboration with other federal agencies and the private sector, to develop, update, and implement a supply chain risk management strategy to ensure the security of the communications and information technology products and services purchased by the federal government. It then directs the Federal Acquisition Regulatory Council (FAR Council) to use its existing authority over federal government procurements to implement the strategy, in much the same way as efforts already under way at the Department of Defense and DHS as part of Initiative 11 of the Comprehensive National Cybersecurity Initiative (CNCI).

Homeland Security Presidential Directive-23 explained the need for supply chain risk management for government information technology procurements:

> *Globalization of the commercial information and communications technology marketplace provides increased opportunities for those intent on harming the United States by penetrating the supply chain to gain unauthorized access to data, alter data, or interrupt communications. Risks stemming from both the domestic and globalized supply chain must be managed in a strategic and comprehensive way over the entire lifecycle of products, systems and services. Managing this risk will require a greater awareness of the threats, vulnerabilities, and consequences associated with acquisition decisions; the development and employment of tools and resources to technically and operationally mitigate risk across the lifecycle of products (from design through retirement); the development of new acquisition policies and practices that reflect the complex global marketplace; and partnership with industry to develop and adopt supply chain and risk management standards and best practices."*[32]

The Committee agrees with this assessment.

Section 253 would create a flexible and comprehensive approach, in partnership with industry, to confront these risks and to ensure that there is greater security built into critical federal networks and systems. Developing a single, unified, approach to this problem will be less burdensome for industry than myriad agency policies developed ad hoc. In fact, the FAR Council is currently considering

[32] The Comprehensive National Cybersecurity Initiative. http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

three cases that propose cybersecurity related changes to the FAR.[33]

The Committee believes this section will result in a prioritization of security practices based on the sensitivity of the systems, avoiding a prescriptive "one-size-fits all" solution. Moreover, the provision recognizes that better security often comes from the private sector, and requires the strategy "to the maximum extent practicable, promote the ability of federal agencies to procure authentic commercial off the shelf information and communications technology products and services from a diverse pool of suppliers." This is further echoed in the requirement in subsection (d) that the strategy "be consistent with the preferences for the acquisition of commercial items under section 2377 of title 10, United States Code, and section 314B of the Federal Property and Administrative Services Act of 1949 (41 U.S.C. 264b)."

The Committee believes that increasing the security of IT products and services sold to the federal government will help promote increased security in the private sector. On June 15, 2010, the Committee heard testimony from witnesses representing electric and telecommunications companies arguing that Section 253 will help their sectors improve security because of the effect of the government's purchasing power throughout the market. Sara Santarelli, Chief Network Security Officer at Verizon testified, "We would like to see the government definitely drive [security controls] into . . . equipment providers so that as we take that equipment and build networks and applications, that equipment [incorporates those] security requirements."

ENHANCING THE CYBERSECURITY WORKFORCE

One of the Federal government's biggest challenges in providing cybersecurity leadership is finding the qualified people necessary to do the job. The need for cybersecurity experts is growing rapidly in both the public and private sector. The government must be competitive with the private sector and other institutions if it is to attract the talent it will need over the coming decades. According to a 2009 report by the Partnership for Public Service, "[the] federal government will be unable to combat [cyber] threats without a more coordinated, sustained effort to increase cybersecurity expertise in the federal workforce."[34] The report cites fragmented leadership and a lack of consistent guidance to hiring managers as key culprits in the government's inability to recruit and retain highly skilled cyber experts.

The Federal government must have a strategic, long-term plan to get federal agencies the staff they need to perform their cyberspace mission. S. 3480 would require the Office of Personnel Management (OPM) to assess the state of readiness of the federal workforce and to identify areas of improvement or gaps that need to be addressed.

---

[33] There are three cybersecurity cases currently pending before the FAR Council—FAR Case 2009–032, Sharing Cyber Threat Information; FAR Case 2009–030, Safeguarding Unclassified Information; FAR Case 2008–019, Authentic IT Products.

[34] Partnership for Public Service, "Cyber In-security: Strengthening the Federal Cybersecurity Workforce." July 2009 at 1. http://www.ourpublicservice.org/OPS/publications/viewcontentdetails.php?id=135.

OPM's existing occupation classifications do not accurately reflect the cyber-related positions currently within the government or those needed in the future. The Committee has learned that program managers seeking to hire individuals with a certain cyber skill set find that they are unable to advertise for the position or specific qualifications they need and instead must adopt the job description to fit the current classifications. Thus, S. 3480 would direct OPM to develop comprehensive occupation classifications not only for the positions in existence for work being done today, but also to assist agencies in developing career paths for employees so we may retain them in federal government service. This career path would include training and development opportunities.

The Committee believes that the federal government must develop a pipeline of capable students in the fields of science, technology, engineering, and mathematics to provide the workforce it will need in the future. Unfortunately, the number of degrees awarded in computer science and other technical fields is declining while our need for professionals with that expertise is growing. To begin to address this need, S. 3480 would direct the Department of Education working with state and local governments and other entities, to develop curriculum standards, guidelines, and recommended courses to address cyber safety, cybersecurity, and cyber ethics for students in kindergarten through grade twelve, as well as undergraduate, graduate, vocational, and technical institutions.

In addition, S. 3480 would create a National Cyber Challenge to help identify potential candidates with badly needed, highly specialized skills. Such challenges have already been used by government agencies, academic institutions, and private sector companies with considerable success. These challenges test participants' abilities to exploit software and hardware weaknesses, crack encrypted codes, and defend against cyber attacks. Some of the participants who won these challenges were high-school students who attended schools with no computer science program and who otherwise might not have readily come to a recruiter's attention. The national challenge would greatly assist in recruiting individuals with world-class skills to help keep our nation's critical infrastructure and government agencies secure.

III. Legislative History

On June 10, 2010, Senators Lieberman, Collins and Carper introduced S. 3480, which was referred to the Senate Committee on Homeland Security and Governmental Affairs.

The Committee held a hearing on June 15, 2010, titled: "Protecting Cyberspace as a National Asset: Comprehensive Legislation for the 21st Century." The Committee received testimony from Philip R. Reitinger, Deputy Under Secretary, National Protection and Programs Directorate, U.S. Department of Homeland Security; Frances Fragos Townsend, Chairwoman of the Board, Intelligence and National Security Alliance; Alan Paller, Director of Research, SANS Institute; Steven T. Naumann, Vice President, Wholesale Market Development, Exelon Corporation; and Sara C. Santarelli, Chief Network Security Officer, Verizon Communications Inc.

The Committee considered S. 3480 on June 24, 2010. The Committee adopted by voice vote a substitute amendment, which made both substantive and technical edits, offered by Senators Lieber-

man, Collins and Carper. The substitute amendment clarified the federal government's responsibility to protect privacy, civil liberties, and proprietary information throughout the bill. It also added identity management and authentication as an area of responsibility of the Director of the White House Office of Cyberspace Policy, and transferred to that Office the responsibility for the communications-related national security and emergency preparedness functions currently residing with the White House Office of Science and Technology Policy.

The substitute amended Section 249, which establishes the "National Cyber Emergency" authority, in three ways. First, it required Congressional approval for the President to extend the application of emergency measures beyond 120 days. Second, in order to ensure that owners and operators of critical infrastructure do not have a disincentive to propose alternative security measures during an emergency, the amendment provides liability protections equivalent to those associated with directed measures if the Director of the NCCC affirmatively determines that the measures are at least as effective as those mandated by the government. Third, it makes clear that a declaration of a National Cyber Emergency does not give the government authority to take certain actions, including compelling disclosure of information not otherwise authorized by law, conducting surveillance, and taking over the operations of privately owned critical infrastructure networks.

The substitute also clarified the definition of covered critical infrastructure by adding language to make more explicit the factors to be considered in the designation of such critical systems. Lastly, the term "cyber vulnerability" was changed to "cyber risk" to better reflect language used in the information technology industry and avoid possible confusion.

The Committee ordered the bill favorably reported, as amended, by voice vote. Members present for the votes on both the substitute amendment and the bill were Senators Lieberman, Levin, Akaka, Carper, Pryor, Kaufman, Collins, Coburn, and McCain.

IV. SECTION-BY-SECTION ANALYSIS

Section 1. Short Title

The short title of the bill is the "Protecting Cyberspace as a National Asset Act of 2010."

Section 2. Table of Contents

Section 2 provides the table of contents for this Act.

Section 3. Definitions

Section 3 defines the following terms: appropriate congressional committee, critical infrastructure, cyberspace, director, federal agency, federal information infrastructure, incident, information infrastructure, information security, information technology, intelligence community, key resources, National Center for Cybersecurity and Communications, national information infrastructure, national security system, national strategy, office, resiliency, risk, and risk-based security.

TITLE I. OFFICE OF CYBERSPACE POLICY

Section 101. Establishment of the Office of Cyberspace Policy

Section 101 establishes an Office of Cyberspace Policy ("the Office") within the Executive Office of the President (EOP). The Section would give the Office the responsibility for developing a national strategy to increase the security and resiliency of cyberspace as well as for overseeing, coordinating and integrating all policies and activities of the federal government related to the security and resiliency of cyberspace.

Section 102. Appointment and responsibilities of the Director

Section 102 would require the President to appoint, and the Senate to confirm, the Director of the Office. The Director would advise the President on all cybersecurity matters, work with federal agencies and other EOP offices to ensure the implementation of the national strategy, coordinate the development of regulations and standards applicable to the national information infrastructure by federal agencies, and resolve any interagency disputes. The Director would also ensure that cybersecurity policies safeguard privacy and civil liberties.

Section 103. Prohibition on political campaigns

Section 103 would prohibit the Director of Cyberspace Policy from participating in certain political activities.

Section 104. Review of federal agency budget requests relating to the national strategy

Section 104 would require the Director of Cyberspace Policy to review each federal agency's budget submission to the Office of Management and Budget (OMB) to determine the adequacy of the request with respect to the implementation of the national strategy and to make recommendations to the Director of OMB based on the review. The Director of Cyberspace Policy would play a crucial role in the budget process, ensuring that agency budgets reflect the goals and objectives outlined in the National Strategy.

Section 105. Access to intelligence

Section 105 would give the Director of Cyberspace Policy access to any information possessed by a federal agency that is relevant to cybersecurity policy, regardless of the information's level of classification.

Section 106. Consultation

Section 106 states that the Director of Cyberspace Policy may consult with any Presidential and other advisory bodies while executing the responsibilities of the Office.

Section 107. Reports to Congress

Section 107 would require the Director of Cyberspace Policy to report to Congress annually on the activities carried out by the Office of Cyberspace Policy. The section would require the Director to submit an unclassified and publicly available version of the report, although the Committee anticipates that the Director may also need to attach a classified, non-public annex.

TITLE II. NATIONAL CENTER FOR CYBERSECURITY AND COMMUNICATIONS

Section 201. Cybersecurity

Section 201 would amend Title II of the Homeland Security Act (HSA) of 2002 to add the sections described below.

New Section 241 of the HSA

Section 241 would define the following terms: agency information infrastructure, covered critical infrastructure, cyber risk, federal information infrastructure, incident, information infrastructure, information security, information sharing and analysis center, information system, intelligence community, management controls, national cyber emergency, national information infrastructure, operational controls, sector-specific agency, sector coordinating councils, security controls, small business concern, and technical controls.

New Section 242 of the HSA

Section 242 would establish a National Center for Cybersecurity and Communications (NCCC or the Center) within the Department of Homeland Security. The Center would be headed by a Director appointed by the President and confirmed by the Senate. The Director would report directly to the Secretary of Homeland Security and serve as the principal advisor to the Secretary on cybersecurity and communications matters. The Director would also regularly advise the President regarding the security of federal government networks. The Center would have at least two Deputy Directors, one responsible for coordination with DHS's Office of Infrastructure Protection and one responsible for coordination with the Intelligence Community. The Center would also have staff detailed from the Departments of Defense, Justice, and Commerce as well as the intelligence community and the National Institute of Standards and Technology (NIST). It would also have a full-time Chief Privacy Officer who would report to the Director.

The Director would be responsible for leading the federal effort to secure, protect, and ensure the resiliency of the information infrastructure of the United States. The Director's specific responsibilities would include: assisting in the identification, remediation, and mitigation of vulnerabilities; providing dynamic, comprehensive, and continuous situational awareness; conducting risk-based assessments; assisting NIST in developing standards; providing agencies with mandatory security controls to mitigate and remediate vulnerabilities; developing policies and guidance for federal procurements; assisting with international engagement; overseeing the development, implementation, and management of external access points for federal networks; establishing, developing and overseeing capabilities and operations within the United States Computer Emergency Readiness Team (US–CERT); fostering collaboration with federal, state, and local governments; and overseeing the operations of the National Communications System.

As a direct report to the Secretary, the National Center for Cybersecurity and Communications would be an operational component with the Department, akin to the Transportation Security Administration, Customs and Border Protection, and the United States Secret Service. This would allow the NCCC to manage its

own hiring, procurement, and security, ensuring these functions are tailored to the needs of the Center and are responsive to the Director.

The two statutory deputies reflect the unique mission of the Center. The links among physical infrastructure protection, cybersecurity, and communications systems are considerable—and growing—and the requirement that one deputy have expertise in physical infrastructure protection would facilitate coordination across these areas. The intelligence-focused deputy, which the Committee assumes would be detailed from the National Security Agency, would ensure that the knowledge and expertise that resides in the intelligence community is integrated into the NCCC from the outset.

The Committee places critical importance on safeguarding privacy rights and civil liberties. The bill would create a full-time Privacy Officer for the Center to ensure that privacy and civil liberties are taken into account in every aspect of Center's policy and operations. The Committee encourages the Privacy Officer to regularly engage with the DHS Chief Privacy Officer, the White House Office of Cyberspace Policy, and non-governmental privacy and civil liberties experts to share information and ensure coordination.

New Section 242 also authorizes the Director to analyze the budgets of other federal agencies and make recommendations to OMB and the White House Office of Cyberspace Policy regarding the adequacy of the proposed budgets to secure federal networks. The NCCC would have relevant information on the state of the federal information infrastructure which would give it a unique ability to provide input on the adequacy of agency budget requests.

New Section 243 of the HSA

Section 243 would require the Director of the Center and the Assistant Secretary for Infrastructure Protection to coordinate on matters regarding the security and resiliency of the nation's critical infrastructure.

New Section 244 of the HSA

Section 244 would codify the United States Computer Emergency Readiness Team (US–CERT) within the NCCC. US–CERT would be responsible for the collection, coordination, and dissemination of information regarding risks to the federal information infrastructure and the enhancement of the security of the national information infrastructure. US–CERT would serve as the primary point of contact within the NCCC for other federal agencies, state and local governments, and the private sector.

US–CERT would provide analysis and report to federal agencies on the security of their networks; provide continuous, automated monitoring of the federal information infrastructure at the external access points; develop, recommend, and deploy security controls; support federal agencies in conducting risk assessments; develop predictive analysis tools; and aid in the detection of and warn owners/operators of the national information infrastructure regarding risks. US–CERT would designate a principal point of contact for each federal agency in order to maintain regular communication and respond to inquiries or requests.

New Section 245 of the HSA

Section 245 would give the Director of the NCCC access to any information possessed by a federal agency that is relevant to the execution of the responsibilities of the position.

The section would also authorize the Director to conduct risk-based operational evaluations (known as "red teaming" and "blue teaming") to evaluate the security of the federal information infrastructure. If the Director determines through the operational evaluation that a federal agency is not in compliance with federal guidelines, the Director, working in conjunction with the head of the agency, may direct the implementation of corrective measures and mitigation plans. If the agency fails to take the directed corrective measures and this failure presents a significant risk to the federal information infrastructure, the Director may direct the isolation of the agency's information infrastructure, consistent with the contingency or continuity of operations plans applicable to that agency, until the agency takes necessary corrective measures.

New Section 246 of the HSA

Section 246 would give the Director of the NCCC responsibility for developing information sharing programs between and among federal agencies, state and local governments, the private sector, and international partners. The Center would establish policies and procedures for sharing classified and unclassified information relevant to the security of the federal and national information infrastructure, including threats, vulnerabilities, incidents, and anomalous activities. The policies and procedures would establish mechanisms for sharing the information, offer guidance on what information should be shared, and protect the information from disclosure.

The Committee expects the Director of the Center to develop standard operating procedures for sending and receiving information from agencies; protocols for how information would be requested; and how routine and urgent information requests are distinguished. The Director should also ensure that each Federal agency has continual access to the agency data collected by US–CERT, including raw data.

This section would require owners and operators of covered critical infrastructure to report to the NCCC significant breaches of their networks that could lead to the disruption of the critical functions of the covered critical infrastructure. The section also directs the NCCC to develop guidance on the form and content of these incident reports. In so doing, the Committee expects the guidelines will help avoid overly burdensome notifications on routine threats and focus reporting on only those incidents that could undermine the reliable operation of the system and cause a catastrophe. The bill, however, explicitly clarifies that this requirement does not affect the Wiretap Act, the Electronic Communications Privacy Act, or the Foreign Intelligence Surveillance Act, or otherwise authorize the Department to compel the disclosure of information from a private sector entity.

New Section 247 of the HSA

Section 247 would direct the Director of the NCCC to engage regularly with standards setting bodies to encourage the development

of, and recommend changes to, cybersecurity standards and guidelines. The Director would also establish a program to promote cybersecurity best practices and provide technical assistance relating to the implementation of best practices, and related standards and guidelines, for securing the national information infrastructure. The section directs that to the extent practicable, these best practices should be based on existing standards developed by the private sector or standard setting bodies. The Committee understands that often cybersecurity standards are written in a manner that only technical experts can implement. The Committee expects that best practices targeted at the national information infrastructure will be prioritized, easily understandable or accompanied by implementation guidance, and informed by both classified and unclassified threat information analyzed by the Center.

New Section 248 of the HSA

Section 248 would require the Director to work with the private sector and relevant sector-specific agencies to identify and evaluate cyber risks to covered critical infrastructure on a sector-by-sector basis. The section would require the Director to complete this evaluation and report to Congress on these efforts within 120 days of the passage of this Act.

The section then would require the Director to work with the private sector and relevant sector-specific agencies to issue interim final regulations establishing risk-based security performance requirements to secure covered critical infrastructure against identified cyber risks. The NCCC would inform owners and operators of covered critical infrastructure of identified vulnerabilities. The owners and operators would then inform the Director of which security measures they intend to implement to meet the performance requirements. Owners and operators would have the flexibility to implement any security measure that the Director determines satisfies the security performance requirements. The Director, however, would not have the authority to mandate any specific security measure—only that the measures selected by the owners and operators meet the applicable risk-based security performance requirements. Consistent with any applicable treaty obligations, the Director would also work with owners and operators of critical infrastructure outside the United States to inform them of cyber risks and appropriate security measures.

New Section 249 of the HSA

Section 249 states that if the President determines there is a threat of an actual or imminent effort to exploit cyber risks to covered critical infrastructure, the President may declare a National Cyber Emergency, with notification to Congress and owners and operators of affected covered critical infrastructure. The notification to Congress must include the nature of the threat, the reason existing security measures are deficient, and the proposed emergency measures needed to address the threat. If the President exercises this authority, the Director of the NCCC could issue mandatory emergency measures necessary to preserve the reliable operation of covered critical infrastructure. Owners and operators of the covered critical infrastructure would be allowed to propose and implement alternative security measures if the Director determined that these

proposed measures were as effective as the directed measures. Emergency declarations could be extended by the President in 30-day increments; however, Congressional approval would be required for any extension of a National Cyber Emergency beyond 120 days. Owners and operators of covered critical infrastructure who comply with the requirements could, in certain circumstances, receive liability protections that range from limitations on punitive and non-economic damages to indemnifications by the United States Government for damages attributable to the implementation of certain security measures.

The Committee does not intend for the exercise of any authority provided by this section to preclude owners and operators from taking other actions to secure their systems, so long as they implement the directed measures or approved alternatives and the additional measures do not undermine the directed or approved alternative measures.

New Section 250 of the HSA

Section 250 would require owners and operators of covered critical infrastructure to certify annually and in writing to the Director of the Center that they are in compliance with the security requirements established under Section 249. The section would authorize the Director to perform evaluations of the covered infrastructure to determine compliance. The Committee believes the Director of the Center should, where possible, utilize existing federal resources to assist in the evaluations. Failure to comply with the regulations could result in civil penalties. Owners and operators of covered critical infrastructure who submit to DHS evaluations, successfully demonstrate compliance with their approved security measures during the evaluation, and can prove compliance at the time of any breach would receive protection from punitive and certain non-economic damages associated with that breach.

New Section 251 of the HSA

Section 251 would require the NCCC to protect from public disclosure sensitive information submitted to the Center and to issue guidelines detailing how information, including information regarding threats, vulnerabilities, and incidents, would be shared with appropriate government and private sector partners.

New Section 252 of the HSA

Section 252 would require the heads of each sector-specific agency and the heads of other federal agencies with responsibilities for regulating covered critical infrastructure to coordinate with the Director of the Center on activities related to the security and resiliency of the national information infrastructure. The section directs the Director of the Center and heads of agencies with sector-specific responsibilities to avoid duplication in reporting requirements wherever possible. These agencies would also have to coordinate with the Director prior to establishing any requirements or other measures related to the security of the national information infrastructure to ensure, to the maximum extent practicable, that the federal government takes a coordinated approach to any regulations or other matters related to cybersecurity.

New Section 253 of the HSA

Section 253 requires the Secretary of DHS, with other federal agencies and the private sector, to develop, update, and implement a supply chain risk management strategy that would ensure the security of the communications and information technology products and services purchased by the federal government. The Federal Acquisition Regulatory Council would be required to amend the Federal Acquisition Regulation to implement the supply chain risk management strategy. The section maintains existing preference for the procurement of commercial off-the-shelf products and services.

TITLE III. FEDERAL INFORMATION SECURITY MANAGEMENT

Section 301. Coordination of Federal Information Policy

Section 301 would amend the Federal Information Security Management Act of 2002 (FISMA) by striking subchapters II and III of chapter 35 of Title 44, United States Code, (44 U.S.C. §§ 3541, et seq.) and inserting the following sections. Many of the original FISMA requirements are retained in this language. The section-by-section analysis below refers to the new sections of Title 44, as amended by this bill.

New Section 3550. Purposes

Section 3550 states that the purpose of Title III is to provide a comprehensive risk-based framework that enhances the effectiveness of information security controls in the federal information infrastructure; recognizes the highly networked nature of the current federal information infrastructure environment; and provides for the development and maintenance of controls required to protect the federal information infrastructure.

New Section 3551. Definitions

Section 3551 would define the following terms: agency information infrastructure, automated and continuous monitoring, incident, information infrastructure, information security, information technology, management controls, national security system, operational controls, risk, risk-based security, security controls, and technical controls.

New Section 3552. Authority and functions of the National Center for Cybersecurity and Communications

Section 3552 would task the Director of the NCCC with the responsibility for developing, overseeing, and enforcing information security throughout the federal government, a task previously assigned to OMB's Office of Electronic Government and Information Technology. Specifically, the Director of the NCCC would have responsibility for providing agencies with prioritized risk-based security controls that would mitigate and remediate vulnerabilities, attacks, and exploitations. In addition, this section would require the Director of the NCCC to ensure agencies comply with government-wide policies and to review the effectiveness of agency information security programs at least annually.

New Section 3553. Agency responsibilities

Section 3553 would require agency heads to follow NCCC policies and to develop and maintain effective risk-based information security programs. In order to accomplish this, the section would require each agency head to delegate to a senior official, known as a Chief Information Security Officer (CISO), the authority to develop, oversee, and enforce risk-based information security policies that are integrated into the strategic and operational processes of the agency. The CISO's authority would extend to the entire agency, including contractors operating on behalf of the agency. To the extent possible, this section requires the CISO to automate their agency's defenses to detect, report, and respond to security incidents. The section would shift resources away from the wasteful, paperwork-laden compliance process required by current law and emphasize active detection and prevention of threats. Specifically, each agency would have to adopt an agency-wide security program, which would be approved by the NCCC and include the following: risk-based vulnerability assessments and penetration tests on agency networks; procedures to ensure that information security vulnerabilities are remediated in a timely fashion; role-based security awareness training for employees; automated and continuous monitoring of network defenses; and plans and procedures to ensure the continuity of operations for information systems that support the operations and assets of the agency. This section would allow CISOs to mandate more stringent standards than those required by the Director of the NCCC. If an incident does occur and information or an information system is compromised, this section would make the CISO responsible for mitigating and remediating the problem as quickly as possible and for reporting any incidents to the appropriate authorities. Finally, this section would require each agency to submit an annual report on the effectiveness of their information security program to Congress, the Government Accountability Office, and the NCCC.

New Section 3554. Annual operational evaluation

Section 3554 would require each agency to conduct annual operational evaluations (also known as "red-teaming" and "blue-teaming") to test the information security program the agency developed pursuant to Section 3553. The operational evaluations would be overseen by the Director of the NCCC and prioritized based on risk. Following an operational evaluation, the CISO would have to submit a risk-based corrective action plan to the Director of the NCCC for mitigating and remediating any vulnerabilities identified as a result of the evaluation. The Director of the NCCC would have fifteen days upon receipt of the plan to approve, disapprove, and comment on the effectiveness of the plan. If the Director approves the plan, then the agency head must ensure that the plan is implemented. In the event that an operational evaluation brings to light severe deficiencies which represent a significant danger to the federal information infrastructure, then the Director of the NCCC may order the isolation of any system from the federal information infrastructure, consistent with the continuity of operations plans applicable to that agency, until the agency takes necessary corrective measures.

New Section 3555. Federal Information Security Taskforce

Section 3555 would establish a Federal Information Security Taskforce within the Executive Branch. The Director of the NCCC would head the Taskforce, whose members would include the Administrator of the Office of Electronic Government; the CISO of every agency; the CISOs of the Army, Navy, and Air Force; representatives from the Office of the Director of National Intelligence, US—CERT, the Intelligence Community Incident Response Center, the Committee on National Security Systems, the National Institute of Standards and Technology, and state and local government; and any other person designated by the chairperson. The Taskforce would serve as the principal interagency forum for agencies to develop and share best practices for enhancing the security of their systems and networks. The Taskforce would be the vehicle through which the Director of the NCCC establishes policies and guidelines to conduct operational evaluations required under Section 3554. In addition, the Taskforce would promote the development and use of standard performance measures for agency information security that are outcome-based, focus on risk management, align with business and program goals of the agency, measure improvements over time, and reduce burdensome compliance measures. The Taskforce would sunset after four years unless extended by Executive Order or an act of Congress.

New Section 3556. Independent assessments

Section 3356 would require Inspectors General to assess the effectiveness of agency information security programs at least every two years.

New Section 3557. Protection of information

Section 3557 would require agencies to protect any information accessed as a result of activities carried out under this Subchapter.

New Section 3558. Department of Defense and Central Intelligence Agency systems

Section 3558 would require the Secretary of Defense and the Director of the Central Intelligence Agency to assume the responsibilities of the Director of the National Center for Cybersecurity and Communications as it relates to their agency information infrastructure. This requirement is consistent with the treatment of the systems of the Department of Defense and the Central Intelligence Agency under current law.

TITLE IV. RECRUITMENT AND PROFESSIONAL DEVELOPMENT

Section 401. Definitions

Section 401 would define the terms cybersecurity mission and federal agency's cybersecurity mission.

Section 402. Assessment of cybersecurity workforce

Section 402 would require the Director of the Office of Personnel Management (OPM) to assess the readiness and capacity of the federal workforce to meet the needs of the federal government's cybersecurity mission. The section would require OPM, within 180 days

of enactment, to develop and implement a comprehensive workforce strategy which includes a five-year plan on recruitment of personnel and ten- and twenty-year projections of workforce needs. The Committee anticipates that OPM would identify areas in the science, technology, engineering, and math fields where additional emphasis needs to be placed to train and recruit candidates.

Section 403. Strategic cybersecurity workforce planning

Section 403 would require the head of each federal agency to develop a strategic cybersecurity workforce plan detailing how the agency plans to recruit, hire, and train necessary cybersecurity personnel. Each agency would have to assess its own needs to determine how to increase and improve their workforce in this area.

Section 404. Cybersecurity occupation classifications

Section 404 would require the Director of OPM to develop and issue comprehensive occupation classifications for federal employees engaged in the cybersecurity mission. The section would require OPM to ensure that the classifications could be used government-wide so as to facilitate the movement of cyber personnel between federal agencies.

Section 405. Measures of cybersecurity hiring effectiveness

Section 405 would require each agency head to develop a system to measure the effectiveness of the agency's recruitment and hiring program.

Section 406. Training and education

Section 406 would require the Director of OPM to establish a cybersecurity awareness program for all federal employees and federal contractors and a program to provide training to improve the technical skills and capabilities of federal employees engaged in the cybersecurity mission. Very few jobs in the federal government do not require access to computers and networks, and as such the Committee believes all employees or contractors should have a baseline of cybersecurity knowledge.

The Director of OPM would be required to develop and implement a strategy to provide federal employees who work in cybersecurity missions with the opportunity to obtain additional education at the expense of the government. The federal government is competing with the private sector for a small pool of highly skilled cyber experts, and the Committee believes that offering educational opportunities that compare with those in the private sector would improve recruitment and retention, as well as improve the overall expertise of the workforce.

The Secretary of Education, working with state and local governments, would be required to develop curriculum standards, guidelines, and recommended courses to address cyber safety, cybersecurity, and cyber ethics for students in kindergarten through grade twelve, as well as undergraduate, graduate, vocational, and technical institutions.

The Director of OPM would also develop strategies and programs to recruit students from undergraduate, graduate, vocational, and technical institutions to serve as federal employees working in cyber missions. The Director of OPM would provide internships

and part-time work opportunities for students from the above institutions.

The Director of the NCCC would be required to establish a program to advance national and statewide cyber competitions and challenges that can identify talented individuals and encourage them to pursue careers in cybersecurity. The challenges should focus on developing and testing student talent in all aspects of cybersecurity with particular focus on hacking, penetration testing, vulnerability assessment, cyber forensics, and offensive and defensive operations.

Section 407. Cybersecurity incentives

Section 407 would require that when the President or an agency head awards bonuses to recognize a federal employee, they must consider the success of that employee in fulfilling the objectives of the National Strategy. The head of an agency would also have to adopt best practices regarding effective ways to educate and motivate employees to demonstrate leadership in cybersecurity.

Section 408. Recruitment and Retention Program for the National Center for Cybersecurity and Communications

Section 408 would direct the Director of the NCCC to establish a program to recruit and retain highly skilled personnel to carry out the mission of the Center. The section would give the Director authority to: directly appoint up to 500 cybersecurity specialists into the competitive service; grant competitive status to individuals previously appointed to an excepted service position; pay up to 20 employees a salary up to level I of the Executive Schedule and, with the direct approval of the Secretary of Homeland Security, up to 5 employees a salary up to that of the Vice President; offer retention bonuses to cybersecurity specialists likely to leave the Department for another federal agency; and to pay entry-level employees a salary higher than currently designated for their position on the General Schedule. These authorities would sunset after 3 years. The creation of the NCCC would be a significant undertaking, and these personnel authorities are intended to provide the Secretary with the flexibility to recruit highly skilled workers quickly and to retain them long-term.

TITLE V. OTHER PROVISIONS

Section 501. Cybersecurity research and development

Section 501 would amend the Homeland Security Act of 2002 to add a new Section 238 encouraging cybersecurity research and development and a new Section 239 to establish the National Cybersecurity Advisory Council.

New Section 238 of the HSA

Section 238 would create a research and development program within the Science and Technology Directorate of the Department of Homeland Security to improve the security of the nation's information infrastructure. A crucial element of this research and development program would be coordination with the NCCC.

New Section 239 of the HSA

Section 239 would direct the Secretary of Homeland Security to establish the National Cybersecurity Advisory Council to advise the Secretary and the Director of the Center on the implementation of cybersecurity provisions affecting the private sector. The Committee also expects the Council to advise and provide input on other parts of the Department's cybersecurity agenda. Members of the Council would be appointed by the Director and include representatives of covered critical infrastructure; academic institutions with expertise in cybersecurity; federal, state, and local government agencies with expertise in cybersecurity; and a representative of the National Security Telecommunications Advisory Council, the Information Technology Sector Coordinating Council, and the Communications Sector Coordinating Council.

Section 502. Prioritized Critical Information Infrastructure

Section 502 would amend the Homeland Security Act of 2002 to require the Secretary to consider certain cybersecurity factors when establishing the Prioritized Critical Infrastructure List required under section 210E(a)(2). This section would also create a new section 254 in the Homeland Security Act.

New Section 254 of the HSA. Covered critical infrastructure

Section 254 would direct the Secretary of Homeland Security to establish and maintain a list of covered critical infrastructure, based on the Prioritized Critical Infrastructure List established under section 210E(a)(2). These designated systems would be subject to the risk-based security performance requirements established in Title II. The Secretary could add or delete systems or assets from the list established under 210E(a)(2) based on the consideration of cybersecurity. The Secretary would be required to notify the owner or operator of the system or asset added to the list as soon as practicable and afford the owner or operator the opportunity to provide information regarding the appropriateness of adding the system or asset to the list. This section would also establish a redress process for owners and operators of covered critical infrastructure to appeal their designations. While appeals are being considered, entities on the list would be required to comply with any requirements applicable to covered critical infrastructure under Title II.

Section 503. National Center for Cybersecurity and Communications acquisition authorities

Section 503 would give the NCCC the same procurement flexibilities currently available to the Department of Defense, NASA and the Coast Guard that allow narrow exceptions to normal competitive procedures for procurements that may be satisfied by only a limited number of responsible sources, or for follow-on contracts for the continued provision of highly specialized services. In order to ensure that these exceptions are used only when necessary, section 503 requires that these authorities would be subject to justification and approval procedures, and the authorities would terminate three years after the date of enactment of this Act. The Director would have to report on a semiannual basis to Congress on the use of the authority granted under this section.

Section 504. Evaluation of the effective implementation of Office of Management and Budget information security related policies and directives

Section 504 would require an evaluation of existing OMB policies, memoranda, and directives relating to information security to determine how well they have been implemented and to make recommendations for improvement. The Administrator for Electronic Government and Information Technology, in coordination with the Chief Information Officers Council, the Federal Information Security Taskforce created in Title III, and the Council of Inspectors General on Integrity and Efficiency, would conduct the evaluation, which would be delivered to Congress. This section specifies that the review should include existing policies on file sharing technology, privacy provisions, and breaches of Personally Identifiable Information, among other information security-related policies.

V. Regulatory Impact and Evaluation

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill. S. 3480 would require owners and operators of the nation's most critical infrastructure to comply with new risk-based security requirements. The Committee agrees with Congressional Budget Office's (CBO) assessment, noted in its cost estimate included in section VI below, that although the new federal regulations would impose intergovernmental and private-sector mandates as defined in the Unfunded Mandates Reform Act, the cost of complying with the regulatory requirements in the bill is dependent on future regulations and therefore cannot be accurately estimated at this time. However, the Committee does not agree with CBO's assessment that more than 50,000 companies could be subject to these requirements. The bill specifically states that the requirements will only apply to systems or assets that if disrupted or destroyed would cause regional or national catastrophic consequences, and the Committee does not believe there are 50,000 entities that will meet this high bar. Moreover, the risk-based performance requirements are designed to apply only to particularly critical systems or assets and not entire companies.

VI. Congressional Budget Office Cost Estimate

November 17, 2010.

Hon. Joseph I. Lieberman,
Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has prepared the enclosed cost estimate for S. 3480, the Protecting Cyberspace as a National Asset Act of 2010.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Matthew Pickford.

Sincerely,

Douglas W. Elmendorf.

Enclosure.

S. 3480—Protecting Cyberspace as a National Asset Act of 2010

Summary: S. 3480 would amend the Federal Information Security Management Act of 2002 (FISMA) to strengthen and coordinate security controls over computer information systems across federal civilian agencies. In addition, the legislation would aim to increase the security of privately owned computer networks for online communication and prevent intentional disruptions of such networks. S. 3480 would establish new offices, require additional testing of computer systems, and provide federal agencies with new authorities and responsibilities related to information security.

Based on information from the Department of Homeland Security (DHS), the Office of Management and Budget (OMB), and other major agencies involved in cybersecurity, CBO estimates that implementing S. 3480 would cost $1.5 billion over the 2011–2015 period, assuming appropriation of the necessary amounts. Most of those funds would be spent on salaries, expenses, and computer hardware and software.

The bill would, under certain circumstances, indemnify owners of critical infrastructure who implement emergency-response plans required by the federal government. CBO estimates that this authority would increase direct spending by $10 million over the 2011–2020 period to pay claims against the U.S. government; therefore, pay-as-you-go procedures apply. Enacting the legislation would not affect revenues.

S. 3480 would impose intergovernmental and private-sector mandates, as defined in the Unfunded Mandates Reform Act (UMRA), on owners and operators of information systems designated as critical infrastructure by DHS. Owners and operators of such systems would have to comply with new security standards and procedures. The bill also would impose a mandate by limiting the damages that users of critical infrastructure can seek from owners and operators of such systems for incidents related to cyber risks.

Because the cost to comply with new security standards would depend on future regulations and because of uncertainty about the number of such claims that would be filed in the absence of this legislation, CBO cannot determine whether the aggregate cost of the mandates in the bill would exceed the annual thresholds established in UMRA for intergovernmental or private-sector mandates ($70 million and $141 million in 2010, respectively, adjusted annually for inflation).

CBO has not reviewed provisions of the bill that would allow the President to declare a national emergency and implement emergency-response and restoration plans. Section 4 of UMRA excludes from the application of that act any legislative provisions that are necessary for national security. CBO has determined that those provisions fall within that exclusion.

Estimated Cost to the Federal Government: The estimated budgetary impact of S. 3480 is shown in the following table. The costs of this legislation fall within budget functions 050 (national defense) and 800 (general government).

	By fiscal year, in millions of dollars—					
	2011	2012	2013	2014	2015	2011–2015
CHANGES IN SPENDING SUBJECT TO APPROPRIATION[a]						
Changes to Information Security Management:						
Estimated Authorization Level	100	175	225	300	325	1,125
Estimated Outlays	80	160	215	285	320	1,060
National Center for Cybersecurity and Communications:						
Estimated Authorization Level	50	50	51	52	53	256
Estimated Outlays	27	44	49	50	51	221
Office of Cyberspace Policy:						
Estimated Authorization Level	10	20	30	31	32	123
Estimated Outlays	8	18	28	30	31	115
Other Provisions:						
Estimated Authorization Level	20	20	20	20	20	100
Estimated Outlays	19	20	20	20	20	99
Total Changes:						
Estimated Authorization Level	180	265	326	403	430	1,604
Estimated Outlays	134	242	312	385	422	1,495

[a] S. 3480 also would increase direct spending by $10 million over the 2016–2020 period, CBO estimates, because of a provision that would, under certain circumstances, indemnify owners of critical infrastructure who comply with government-ordered procedures during a cyber emergency.

Note: Components may not sum to totals because of rounding.

Basis of Estimate: For this estimate, CBO assumes that the bill will be enacted in calendar year 2010, that the necessary amounts will be appropriated each year, and that spending will follow historical patterns for salaries and expenses related to securing federal information systems. CBO estimates that implementing S. 3480 would cost about $1.5 billion over the 2011–2015 period.

Changes to information security management

Under S. 3480, agencies would be required to perform new activities, including:

- Automated monitoring of systems to secure information;
- Testing of information security controls;
- Evaluating information security programs and practices; and
- Establishing a Federal Information Security Task Force.

Most of the provisions of the bill would expand practices already being carried out by the federal government under FISMA. In 2009, federal agencies spent nearly $7 billion on such activities. That amount includes about $300 million for certification and accreditation activities (the processes used by all federal agencies to assess, test, and accept the security controls that protect information systems). FISMA also sets forth a comprehensive framework for ensuring that security controls for information resources that support federal operations and assets are effective. Specifically, FISMA requires the head of each agency to provide protections that would be commensurate with the risk and magnitude of harm that would result from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information and systems used or operated by each agency.

Based on information from OMB and other selected agencies, CBO estimates that when fully implemented, the new activities specified in S. 3480 would increase federal spending for FISMA activities by about 4 percent—about $300 million annually. CBO expects that it would take about four years to reach that level of effort for the thousands of federal computer systems currently operating. Over the 2011–2015 period, we estimate that implementing

those new requirements and authorities would cost about $1 billion, assuming appropriation of the necessary amounts.

National Center for Cybersecurity and Communications

Section 201 would establish the National Center for Cybersecurity and Communications (NCCC) within the Department of Homeland Security. The new center would be responsible for leading DHS's efforts to secure federal civilian networks and work with state and local governments and the private sector to secure the nation's information infrastructure. The bill would transfer the authorities, personnel, and other assets of DHS's National Cybersecurity Division, the Office of Emergency Communications, and the National Communications System to the NCCC.

Although the bill would transfer existing assets and funds to the NCCC, CBO anticipates that the mission of the new NCCC would require additional funding to implement. In particular, the bill would require more extensive testing of federal and private information systems. In its 2011 budget justification, DHS outlined a plan to spend approximately $10 million to conduct 27 assessments of the federal government's information systems. Based on that information, CBO estimates that conducting the cyber assessments envisioned by the bill would cost an additional $220 million over the 2011–2015 period, assuming appropriation of the necessary amounts.

Office of Cyberspace Policy

The Executive Office of the President currently employs a coordinator to manage cybersecurity policies. Title I would expand that role and establish an Office of Cyberspace Policy within the Executive Office of the President. The office would advise the President and help coordinate all cybersecurity regulations, standards, and strategies.

Based on information provided by OMB and the cost of similar offices and programs, CBO estimates that creating the new office would cost about $30 million a year once fully implemented. We expect that the office would steadily expand its budget and staff over three years before it reached that level of effort and estimate that implementing the title would cost $115 million over the 2011–2015 period.

Other provisions

The legislation also would require federal agencies to:

- Assess the skills of information security employees;
- Prepare plans to train information security workers; and
- Establish a National Cybersecurity Advisory Council.

Based on information from DHS and OMB, CBO estimates that implementing those provisions would cost about $20 million annually over the 2011–2015 period.

Direct spending

Under the bill, the Director of the NCCC would be authorized to require owners of critical infrastructure (assets essential to society and the economy, including facilities for energy production, telecommunications, public health, and food and water supply) to implement response plans if a national cyber emergency was declared

by the President. Although the probability is very low, such a plan could involve an interruption of service in the telecommunications or electric power sectors. Section 201 would indemnify the owners of such infrastructure in civil actions if implementation of those response plans resulted in the serious physical injury or death of an individual or substantial damage or destruction of an individual's primary residence. Any claims against the government related to indemnifying such entities would be paid from the Judgment Fund (a permanent, indefinite appropriation for claims and judgments against the United States) and would be considered direct spending.

CBO has determined that cyber attacks on electrical utilities and telecommunications providers would present the biggest potential for liability under this section because an interruption of service in those sectors could affect emergency response services. Because there is no relevant historical data on which to determine the probability of an attack that would trigger the implementation of such plans, CBO consulted with numerous cyber security and cyber insurance experts. CBO based its estimate of the costs of indemnifying entities on information derived from those discussions including the likelihood of a widespread, high-impact cyber event and on an analysis of the potential liability if there was an interruption of electrical power or telecommunications services in a large metropolitan area. Based on that analysis, CBO estimates that enacting this provision would increase direct spending by $10 million over the 2016–2020 period. Since CBO cannot predict the value of claims that might be paid in any particular year, our estimate of the cost represents the sum of a weighted average of payments from the Judgment Fund over the 2016–2020 period. Since CBO anticipates that any potential litigation involving such claims would be lengthy, we estimate that this provision would not affect direct spending over the 2011–2015 period.

Pay-As-You-Go considerations: The Statutory Pay-As-You-Go Act of 2010 establishes budget reporting and enforcement procedures for legislation affecting direct spending or revenues. S. 3480 could affect direct spending by agencies not funded through annual appropriations, such as the Tennessee Valley Authority and the Bonneville Power Administration; therefore, pay-as-you-go procedures apply. CBO estimates, however, that any net increase in annual spending by those agencies would not be significant and enacting the legislation would not affect revenues.

In addition, the bill would affect direct spending because of a provision that would, under certain circumstances, indemnify owners of critical infrastructure who comply with government-ordered procedures during a cyber emergency. CBO estimates that enacting that provision would increase direct spending by $10 million over the 2016–2020 period.

In total, the net budgetary changes in the bill subject to pay-as-you-go procedures would be insignificant over the 2011–2015 period and $10 million over the 2016–2020 period.

Intergovernmental and private-sector impact: S. 3480 contains several intergovernmental and private-sector mandates, as defined in UMRA. Because of uncertainty about the nature or scope of some of the mandates, CBO cannot determine whether the aggregate cost of the mandates in the bill would exceed the annual

thresholds established in UMRA for intergovernmental or private-sector mandates ($70 million and $141 million in 2010, respectively, adjusted annually for inflation).

Mandates that apply to both intergovernmental and private-sector entities

Cyber protection. The bill would impose intergovernmental and private-sector mandates, as defined in UMRA, on owners and operators of information systems designated as critical infrastructure by DHS. Owners and operators of such systems would have to comply with new security standards and reporting requirements. Critical infrastructure could include information systems for public and private transportation systems, police and fire departments, airports, hospitals, electric utilities, health departments, water systems, and financial companies. Based on information from government and industry sources, CBO estimates that more than 50,000 public entities could be subject to the mandates. Further, a study by the Government Accountability Office indicates that the private sector owns more than 85 percent of the nation's critical infrastructure.

The bill would require owners and operators of information systems designated as critical infrastructure to comply with standards for managing cybersecurity risks and to certify in writing that they are in compliance with those standards. Because the costs of complying with the mandate would depend on future regulations, CBO has no basis for estimating the cost of the mandates on public or private-sector entities, primarily because it is not clear which entities would be affected or whether future regulations would differ significantly from current practices.

S. 3480 also would require affected entities to report incidents that could indicate a risk to cybersecurity. CBO estimates that the cost of complying with this mandate to public and private entities would be small relative to the annual thresholds.

Liability limits. The bill also would impose a mandate by limiting the damages that may be recovered from owners and operators of critical infrastructure for incidents related to cyber risks. Compensation for certain damages would only be limited for claims against owners and operators that comply with the cybersecurity standards issued by DHS. Because we are uncertain about both the value of awards in such cases and the number of claims that would be filed in the absence of this legislation, CBO cannot determine whether the cost of the mandate would exceed the annual thresholds for intergovernmental or private-sector mandates.

Provisions excluded under UMRA

CBO has not reviewed provisions of the bill that would allow the President to declare a national cyber emergency and implement emergency-response and restoration plans. Section 4 of UMRA excludes from the application of that act any legislative provisions that are necessary for national security. CBO has determined that those provisions fall within that exclusion.

Estimate prepared by: Federal costs: Matthew Pickford and Jason Wheelock; Impact on state, local, and tribal governments: Elizabeth Cove Delisle; Impact on the private sector: Samuel Wice.

Estimate approved by: Theresa Gullo, Deputy Assistant Director for Budget Analysis.

COMMITTEE COMMENTS REGARDING COST ESTIMATE

The Committee questions portions of the cost estimate prepared by the Congressional Budget Office (CBO). CBO estimated that changes to information security management required by Title III of S. 3480 would increase federal spending for activities under the Federal Information Security Management Act (FISMA) by about 4 percent, or $1 billion over a 5-year period. Yet in 2008, CBO estimated that S. 3474, a bill to amend FISMA that would have placed more burdensome and costly reporting and compliance obligations on federal agencies than does S. 3480, was estimated to increase FISMA spending by only 2 to 3 percent, or $570 million over a 5-year period. The Committee believes that by modernizing FISMA, S. 3480 will reduce both the current cost and the burden of federal information security. The Committee notes that provisions in S. 3480 are far less burdensome on agencies than even those in S. 3474. For example, unlike S. 3474, S. 3480 calls for operational evaluations, rather than more stringent "audits;" allows Inspectors General to leverage existing work rather than begin all evaluations anew; and allows dual-hatting of Chief Information Officers and Chief Information Security Officers. Thus, the Committee believes the FISMA reforms in S. 3480 will drastically decrease burdensome requirements contained in current law, and that any obligations imposed on federal agencies would be less than that associated with S. 3474.

The Committee also questions the cost estimate for the White House Office of Cyberspace Policy. This office will oversee federal cyberspace activities to ensure efficiency and coordination across the federal government, but it will not have an operational role. The Committee expects the Office to be staffed in a manner similar to the National Security Staff—with a mix of full-time employees and detailees—but with a significantly smaller headcount. The Committee does not believe that the estimated cost for the Office of Cyberspace Policy should be two times the current budget for the entire National Security Staff.

VII. CHANGES IN EXISTING LAW MADE BY THE BILL AS REPORTED

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, the following changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

UNITED STATES CODE

* * * * * * *

TITLE 44—PUBLIC PRINTING AND DOCUMENTS

* * * * * * *

CHAPTER 35—CORDINATION OF FEDERAL INFORMATION POLICY

* * * * * * *

SUBCHAPTER II—INFORMATION SECURITY

* * * * * * *

[§ 3531. Purposes

[The purposes of this subchapter are to—

[(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

[(2) recognize the highly networked nature of the current Federal computing environment and provide effective government wide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;

[(3) provide for development and maintenance of minimum controls required to protect Federal information and information systems;

[(4) provide a mechanism for improved oversight of Federal agency information security programs;

[(5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector; and

[(6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

[§ 3532. Definitions

[(a) IN GENERAL.—Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

[(b) ADDITIONAL DEFINITIONS.—As used in this subchapter—

[(1) the term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

[(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

[(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information;

[(C) availability, which means ensuring timely and reliable access to and use of information; and

[(D) authentication, which means utilizing digital credentials to assure the identity of users and validate their access;

[(2) 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, the function, operation, or use of which—

[(A) involves intelligence activities;

[(B) involves cryptologic activities related to national security;

[(C) involves command and control of military forces;

[(D) involves equipment that is an integral part of a weapon or weapons system; or

[(E) is critical to the direct fulfillment of military or intelligence missions provided that this definition does not apply to a system that is used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications);

[(3) the term "information technology" has the meaning given that term in section 11101 of title 40; and

[(4) the term "information system" means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information, and includes—

[(A) computers and computer networks;

[(B) ancillary equipment;

[(C) software, firmware, and related procedures;

[(D) services, including support services; and

[(E) related resources.

[§ 3533. Authority and functions of the Director

[(a) The Director shall oversee agency information security policies and practices, by—

[(1) promulgating information security standards under section 11331 of title 40;

[(2) overseeing the implementation of policies, principles, standards, and guidelines on information security;

[(3) requiring agencies, consistent with the standards promulgated under such section 11331 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

[(A) information collected or maintained by or on behalf of an agency; or

[(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

[(4) 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;

[(5) overseeing agency compliance with the requirements of this subchapter, including through any authorized action under section 11303(b)(5)of title 40, to enforce accountability for compliance with such requirements;

[(6) reviewing at least annually, and approving or disapproving, agency information security programs required under section 3534(b);

[(7) coordinating information security policies and procedures with related information resources management policies and procedures; and

[(8) reporting to Congress no later than March 1 of each year on agency compliance with the requirements of this subchapter, including—

[(A) a summary of the findings of evaluations required by section 3535;

[(B) significant deficiencies in agency information security practices;

[(C) planned remedial action to address such deficiencies; and

[(D) a summary of, and the views of the Director on, the report prepared by the National Institute of Standards and Technology under section 20(d)(9) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

[(b) Except for the authorities described in paragraphs (4) and (7) of subsection (a), the authorities of the Director under this section shall not apply to national security systems.

[§ 3534. Federal agency responsibilities

[(a) The head of each agency shall—

[(1) be responsible for—

[(A)providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

[(i) information collected or maintained by or on behalf of the 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;

[(B) complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including—

[(i) information security standards promulgated by the Director under section 11331 of title 40; and

[(ii) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and

[(C) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

[(2) ensure that senior agency officials provide information security for the information and information systems that sup-

port the operations and assets under their control, including through—

[(A) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

[(B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under section 11331 of title 40 for information security classifications and related requirements;

[(C) implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and

[(D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented;

[(3) delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including—

[(A) designating a senior agency information security officer who shall—

[(i) carry out the Chief Information Officer's responsibilities under this section;

[(ii) possess professional qualifications, including training and experience, required to administer the functions described under this section;

[(iii) have information security duties as that official's primary duty; and

[(iv) head an office with the mission and resources to assist in ensuring agency compliance with this section;

[(B) developing and maintaining an agencywide information security program as required by subsection (b);

[(C) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3533 of this title, and section 11331 of title 40;

[(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

[(E) assisting senior agency officials concerning their responsibilities under paragraph (2);

[(4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and

[(5) ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions.

[(b) Each agency shall develop, document, and implement an agencywide information security program, approved by the Director under section 3533(a)(5), to provide information security for the in-

formation and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes—

[(1) periodic assessments of the risk and magnitude of the harm 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;

[(2) policies and procedures that—

[(A) are based on the risk assessments required by paragraph (1);

[(B) cost-effectively reduce information security risks to an acceptable level;

[(C) ensure that information security is addressed throughout the life cycle of each agency information system; and

[(D) ensure compliance with—

[(i) the requirements of this subchapter;

[(ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40;

[(iii) minimally acceptable system configuration requirements, as determined by the agency; and

[(iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;

[(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;

[(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of—

[(A) information security risks associated with their activities; and

[(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;

[(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing—

[(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505 (c); and

[(B) may include testing relied on in a [1] evaluation under section 3535;

[(6) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

[(7) procedures for detecting, reporting, and responding to security incidents, including—

[(A) mitigating risks associated with such incidents before substantial damage is done; and

[(B) notifying and consulting with, as appropriate—

[(i) law enforcement agencies and relevant Offices of Inspector General;

[(ii) an office designated by the President for any incident involving a national security system; and

[(iii) any other agency or office, in accordance with law or as directed by the President; and

[(8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

[(c) Each agency shall—

[(1) report annually to the Director, the Committees on Government Reform and Science of the House of Representatives, the Committees on Governmental Affairs and Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of this subchapter, including compliance with each requirement of subsection (b);

[(2) address the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to—

[(A) annual agency budgets;

[(B) information resources management under subchapter 1 [2] of this chapter;

[(C) information technology management under subtitle III of title 40;

[(D) program performance under sections 1105 and 1115 through 1119 of title 31, and sections 2801 and 2805 of title 39;

[(E) financial management under chapter 9 of title 31, and the Chief Financial Officers Act of 1990 (31 U.S.C. 501 note; Public Law 101–576) (and the amendments made by that Act);

[(F) financial management systems under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note); and

[(G) internal accounting and administrative controls under section 3512 of title 31, United States Code,[3] (known as the "Federal Managers Financial Integrity Act"); and

[(3) report any significant deficiency in a policy, procedure, or practice identified under paragraph (1) or (2)—

[(A) as a material weakness in reporting under section 3512 of title 31; and

[(B) if relating to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note).

[(d)(1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of—

[(A) the time periods; and

[(B) the resources, including budget, staffing, and training, that are necessary to implement the program required under subsection (b).

[(2) The description under paragraph (1) shall be based on the risk assessments required under subsection (b)(2)(1).

[(e) Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.

[§ 3535. Annual independent evaluation

[(a)(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

[(2) Each evaluation by an agency under this section shall include—

[(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;

[(B) an assessment (made on the basis of the results of the testing) of compliance with—

[(i) the requirements of this subchapter; and

[(ii) related information security policies, procedures, standards, and guidelines; and

[(C) separate presentations, as appropriate, regarding information security relating to national security systems.

[(b) Subject to subsection (c)—

[(1) for each agency with an Inspector General appointed under the Inspector General Act of 1978 or any other law, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency; and

[(2) for each agency to which paragraph (1) does not apply, the head of the agency shall engage an independent external auditor to perform the evaluation.

[(c) For each agency operating or exercising control of a national security system, that portion of the evaluation required by this section directly relating to a national security system shall be performed—

[(1) only by an entity designated by the agency head; and

[(2) in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

[(d) The evaluation required by this section—

[(1) shall be performed in accordance with generally accepted government auditing standards; and

[(2) may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

[(e) Each year, not later than such date established by the Director, the head of each agency shall submit to the Director the results of the evaluation required under this section.

[(f) Agencies and evaluators shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws and regulations.

[(g)(1) The Director shall summarize the results of the evaluations conducted under this section in the report to Congress required under section 3533(a)(8).

[(2) The Director's report to Congress under this subsection shall summarize information regarding information security relating to national security systems in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

[(3) Evaluations and any other descriptions of information systems under the authority and control of the Director of Central Intelligence or of National Foreign Intelligence Programs systems under the authority and control of the Secretary of Defense shall be made available to Congress only through the appropriate oversight committees of Congress, in accordance with applicable laws.

[(h) The Comptroller General shall periodically evaluate and report to Congress on—

[(1) the adequacy and effectiveness of agency information security policies and practices; and

[(2) implementation of the requirements of this subchapter.

[§ 3536. 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;

[(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; and

[(3) complies with the requirements of this subchapter.

[§ 3537. Authorization of appropriations

[There are authorized to be appropriated to carry out the provisions of this subchapter such sums as may be necessary for each of fiscal years 2003 through 2007.

[§ 3538. Effect on existing law

[Nothing in this subchapter, section 11331 of title 40, or section 20 of the National Standards[1] and Technology Act (15 U.S.C. 278g–3) may be construed as affecting the authority of the President, the Office of Management and Budget or the Director thereof, the National Institute of Standards and Technology, or the head of any agency, with respect to the authorized use or disclosure of information, including with regard to the protection of personal privacy under section 552a of title 5, the disclosure of information under section 552 of title 5, the management and disposition of

records under chapters 29, 31, or 33 of title 44, the management of information resources under subchapter I of chapter 35 of this title, or the disclosure of information to Congress or the Comptroller General of the United States.]

* * * * * * *

SUBCHAPTER III—INFORMATION SECURITY

* * * * * * *

[§ 3541. Purposes

[The purposes of this subchapter are to—

[(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

[(2) recognize the highly networked nature of the current Federal computing environment and provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;

[(3) provide for development and maintenance of minimum controls required to protect Federal information and information systems;

[(4) provide a mechanism for improved oversight of Federal agency information security programs;

[(5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector; and

[(6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

[§ 3542. Definitions

[(a) IN GENERAL.—Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

[(b) ADDITIONAL DEFINITIONS.—As used in this subchapter:

[(1) The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

[(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

[(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

[(C) availability, which means ensuring timely and reliable access to and use of information.

[(2)(A) 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) 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).

[(3) The term "information technology" has the meaning given that term in section 11101 of title 40.

[§ 3543. Authority and functions of the Director

[(a) IN GENERAL.—The Director shall oversee agency information security policies and practices, including—

[(1) developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards promulgated under section 11331 of title 40;

[(2) requiring agencies, consistent with the standards promulgated under such section 11331 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

[(A) information collected or maintained by or on behalf of an agency; or

[(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

[(3) 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;

[(4) overseeing agency compliance with the requirements of this subchapter, including through any authorized action under section 11303 of title 40, to enforce accountability for compliance with such requirements;

[(5) reviewing at least annually, and approving or disapproving, agency information security programs required under section 3544 (b);

[(6) coordinating information security policies and procedures with related information resources management policies and procedures;

[(7) overseeing the operation of the Federal information security incident center required under section 3546; and

[(8) reporting to Congress no later than March 1 of each year on agency compliance with the requirements of this subchapter, including—

[(A) a summary of the findings of evaluations required by section 3545;

[(B) an assessment of the development, promulgation, and adoption of, and compliance with, standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) and promulgated under section 11331 of title 40;

[(C) significant deficiencies in agency information security practices;

[(D) planned remedial action to address such deficiencies; and

[(E) a summary of, and the views of the Director on, the report prepared by the National Institute of Standards and Technology under section 20(d)(10) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

[(b) NATIONAL SECURITY SYSTEMS.—Except for the authorities described in paragraphs (4) and (8) of subsection (a), the authorities of the Director under this section shall not apply to national security systems.

[(c) DEPARTMENT OF DEFENSE AND CENTRAL INTELLIGENCE AGENCY SYSTEMS.—

[(1) The authorities of the Director described in paragraphs (1) and (2) of subsection (a) shall be delegated to the Secretary of Defense in the case of systems described in paragraph (2) and to the Director of Central Intelligence in the case of systems described in paragraph (3).

[(2) The systems described in this paragraph are systems that are operated by the Department of Defense, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Department of Defense.

[(3) The systems described in this paragraph are systems that are operated by the Central Intelligence Agency, a contractor of the Central Intelligence Agency, or another entity on behalf of the Central Intelligence Agency that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Central Intelligence Agency.

[§ 3544. Federal agency responsibilities

[(a) IN GENERAL.—The head of each agency shall—

[(1) be responsible for—

[(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

[(i) information collected or maintained by or on behalf of the 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;

[(B) complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including—

[(i) information security standards promulgated under section 11331 of title 40; and

[(ii) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and

[(C) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

[(2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through—

[(A) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

[(B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under section 11331 of title 40, for information security classifications and related requirements;

[(C) implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and

[(D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented;

[(3) delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including—

[(A) designating a senior agency information security officer who shall—

[(i) carry out the Chief Information Officer's responsibilities under this section;

[(ii) possess professional qualifications, including training and experience, required to administer the functions described under this section;

[(iii) have information security duties as that official's primary duty; and

[(iv) head an office with the mission and resources to assist in ensuring agency compliance with this section;

[(B) developing and maintaining an agencywide information security program as required by subsection (b);

[(C) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3543 of this title, and section 11331 of title 40;

[(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

[(E) assisting senior agency officials concerning their responsibilities under paragraph (2);

[(4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and

[(5) ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions.

[(b) AGENCY PROGRAM.—Each agency shall develop, document, and implement an agencywide information security program, approved by the Director under section 3543(a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes—

[(1) periodic assessments of the risk and magnitude of the harm 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;

[(2) policies and procedures that—

[(A) are based on the risk assessments required by paragraph (1);

[(B) cost-effectively reduce information security risks to an acceptable level;

[(C) ensure that information security is addressed throughout the life cycle of each agency information system; and

[(D) ensure compliance with—

[(i) the requirements of this subchapter;

[(ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40;

[(iii) minimally acceptable system configuration requirements, as determined by the agency; and

[(iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;

[(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;

[(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of—

[(A) information security risks associated with their activities; and

[(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;

[(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing—

[(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505 (c); and

[(B) may include testing relied on in an evaluation under section 3545;

[(6) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

[(7) procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued pursuant to section 3546 (b), including—

[(A) mitigating risks associated with such incidents before substantial damage is done;

[(B) notifying and consulting with the Federal information security incident center referred to in section 3546; and

[(C) notifying and consulting with, as appropriate—

[(i) law enforcement agencies and relevant Offices of Inspector General;

[(ii) an office designated by the President for any incident involving a national security system; and

[(iii) any other agency or office, in accordance with law or as directed by the President; and

[(8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

[(c) AGENCY REPORTING.—Each agency shall—

[(1) report annually to the Director, the Committees on Government Reform and Science of the House of Representatives, the Committees on Governmental Affairs and Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of this subchapter, including compliance with each requirement of subsection (b);

[(2) address the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to—

[(A) annual agency budgets;

[(B) information resources management under subchapter 1 of this chapter;

[(C) information technology management under subtitle III of title 40;

[(D) program performance under sections 1105 and 1115 through 1119 of title 31, and sections 2801 and 2805 of title 39;

[(E) financial management under chapter 9 of title 31, and the Chief Financial Officers Act of 1990 (31 U.S.C. 501 note; Public Law 101–576) (and the amendments made by that Act);

[(F) financial management systems under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note); and

[(G) internal accounting and administrative controls under section 3512 of title 31, (known as the "Federal Managers Financial Integrity Act"); and

[(3) report any significant deficiency in a policy, procedure, or practice identified under paragraph (1) or (2)—

[(A) as a material weakness in reporting under section 3512 of title 31; and

[(B) if relating to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note).

[(d) PERFORMANCE PLAN.—

[(1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of—

[(A) the time periods, and

[(B) the resources, including budget, staffing, and training, that are necessary to implement the program required under subsection (b).

[(2) The description under paragraph (1) shall be based on the risk assessments required under subsection (b)(2)(1).

[(e) PUBLIC NOTICE AND COMMENT.—Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.

[§ 3545. Annual independent evaluation

[(a) IN GENERAL.—

[(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

[(2) Each evaluation under this section shall include—

[(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;

[(B) an assessment (made on the basis of the results of the testing) of compliance with—

[(i) the requirements of this subchapter; and

[(ii) related information security policies, procedures, standards, and guidelines; and

[(C) separate presentations, as appropriate, regarding information security relating to national security systems.

[(b) INDEPENDENT AUDITOR.—Subject to subsection (c)—

[(1) for each agency with an Inspector General appointed under the Inspector General Act of 1978 or any other law, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency; and

[(2) for each agency to which paragraph (1) does not apply, the head of the agency shall engage an independent external auditor to perform the evaluation.

[(c) NATIONAL SECURITY SYSTEMS.—For each agency operating or exercising control of a national security system, that portion of the evaluation required by this section directly relating to a national security system shall be performed—

[(1) only by an entity designated by the agency head; and

[(2) in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

[(d) EXISTING EVALUATIONS.—The evaluation required by this section may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

[(e) AGENCY REPORTING.—

[(1) Each year, not later than such date established by the Director, the head of each agency shall submit to the Director the results of the evaluation required under this section.

[(2) To the extent an evaluation required under this section directly relates to a national security system, the evaluation results submitted to the Director shall contain only a summary and assessment of that portion of the evaluation directly relating to a national security system.

[(f) PROTECTION OF INFORMATION.—Agencies and evaluators shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws and regulations.

[(g) OMB REPORTS TO CONGRESS.—

[(1) The Director shall summarize the results of the evaluations conducted under this section in the report to Congress required under section 3543(a)(8).

[(2) The Director's report to Congress under this subsection shall summarize information regarding information security relating to national security systems in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

[(3) Evaluations and any other descriptions of information systems under the authority and control of the Director of Central Intelligence or of National Foreign Intelligence Programs systems under the authority and control of the Secretary of Defense shall be made available to Congress only through the ap-

propriate oversight committees of Congress, in accordance with applicable laws.

[(h) COMPTROLLER GENERAL.—The Comptroller General shall periodically evaluate and report to Congress on—

[(1) the adequacy and effectiveness of agency information security policies and practices; and

[(2) implementation of the requirements of this subchapter.

[§ 3546. Federal information security incident center

[(a) IN GENERAL.— The Director shall ensure the operation of a central Federal information security incident center to—

[(1) provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;

[(2) compile and analyze information about incidents that threaten information security;

[(3) inform operators of agency information systems about current and potential information security threats, and vulnerabilities; and

[(4) consult with the National Institute of Standards and Technology, agencies or offices operating or exercising control of national security systems (including the National Security Agency), and such other agencies or offices in accordance with law and as directed by the President regarding information security incidents and related matters.

[(b) NATIONAL SECURITY SYSTEMS.—Each agency operating or exercising control of a national security system shall share information about information security incidents, threats, and vulnerabilities with the Federal information security incident center to the extent consistent with standards and guidelines for national security systems, issued in accordance with law and as directed by the President.

[§ 3547. 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;

[(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; and

[(3) complies with the requirements of this subchapter.

[§ 3548. Authorization of appropriations

[There are authorized to be appropriated to carry out the provisions of this subchapter such sums as may be necessary for each of fiscal years 2003 through 2007.

[§ 3549. Effect on existing law

[Nothing in this subchapter, section 11331 of title 40, or section 20 of the National Standards and Technology Act (15 U.S.C. 278g–3) may be construed as affecting the authority of the President, the Office of Management and Budget or the Director thereof, the National Institute of Standards and Technology, or the head of any agency, with respect to the authorized use or disclosure of information, including with regard to the protection of personal privacy under section 552a of title 5, the disclosure of information under section 552 of title 5, the management and disposition of records under chapters 29, 31, or 33 of title 44, the management of information resources under subchapter I of chapter 35 of this title, or the disclosure of information to the Congress or the Comptroller General of the United States. While this subchapter is in effect, subchapter II of this chapter shall not apply.**]**

* * * * * * *

TITLE II—FEDERAL INFORMATION SECURITY MANAGEMENT

* * * * * * *

SEC. 301. COORDINATION OF FEDERAL INFORMATION POLICY.

(a) FINDINGS—Congress finds that—

(1) since 2002 the Federal Government has experienced multiple high-profile incidents that resulted in the theft of sensitive information amounting to more than the entire print collection contained in the Library of Congress, including personally identifiable information, advanced scientific research, and prenegotiated United States diplomatic positions; and

(2) chapter 35 of title 44, United States Code, must be amended to increase the coordination of Federal agency activities and to enhance situational awareness throughout the Federal Government using more effective enterprise-wide automated monitoring, detection, and response capabilities.

(b) 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

SEC. 3550. PURPOSES.

The purposes of this subchapter are to—

(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support the Federal information infrastructure and the operations and assets of agencies;

(2) recognize the highly networked nature of the current Federal information infrastructure and provide effective Government-wide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;

(3) provide for development and maintenance of prioritized and risk-based security controls required to protect Federal information infrastructure and information systems;

(4) provide a mechanism for improved oversight of Federal agency information security programs;

(5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the Nation that are designed, built, and operated by the private sector; and

(6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

SEC. 3551. DEFINITIONS.

(a) IN GENERAL.—Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

(b) ADDITIONAL DEFINITIONS.—In this subchapter:

(1) The term "agency information infrastructure"—

(A) means information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, an agency, including information systems used or operated by another entity on behalf of the agency; and

(B) does not include national security systems.

(2) The term "automated and continuous monitoring" means monitoring at a frequency and sufficiency such that the data exchange requires little to no human involvement and is not interrupted.

(3) The term "incident" means an occurrence that—

(A) actually or potentially jeopardizes—

(i) the information security of an information system; or

(ii) the information the system processes, stores, or transmits; or

(B) constitutes a violation or threat of violation of security policies, security procedures, or acceptable use policies.

(4) The term "information infrastructure" means the underlying framework that information systems and assets rely on to process, transmit, receive, or store information electronically, including programmable electronic devices and communications networks and any associated hardware, software, or data.

(5) 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; and

(C) availability, by ensuring timely and reliable access to and use of information.

(6) The term "information technology" has the meaning given that term in section 11101 of title 40.

(7) The term "management controls" means safeguards or countermeasures for an information system that focus on the management of risk and the management of information system security.

(8)(A) 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) that 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) 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).

(9) The term "operational controls" means the safeguards and countermeasures for an information system that are primarily implemented and executed by individuals, not systems.

(10) The term "risk" means the potential for an unwanted outcome resulting from an incident, as determined by the likelihood of the occurrence of the incident and the associated consequences, including potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident.

(11) The term "risk-based security" means security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to, or modification, of information, including assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability.

(12) The term "security controls" means the management, operational, and technical controls prescribed for an information system to protect the information security of the system.

(13) The term "technical controls" means the safeguards or countermeasures for an information system that are primarily implemented and executed by the information system through mechanism contained in the hardware, software, or firmware components of the system.

SEC. 3552. AUTHORITY AND FUNCTIONS OF THE NATIONAL CENTER FOR CYBERSECURITY AND COMMUNICATIONS.

(a) IN GENERAL.—The Director of the National Center for Cybersecurity and Communications shall—

(1) develop, oversee the implementation of, and enforce policies, principles, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) and subtitle E of title II of the Homeland Security Act of 2002;

(2) provide to agencies security controls that agencies shall be required to be implemented to mitigate and remediate vulnerabilities, attacks, and exploitations discovered as a result of activities required under this subchapter or subtitle E of title II of the Homeland Security Act of 2002;

(3) to the extent practicable—

(A) prioritize the policies, principles, standards, and guidelines promulgated under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), paragraph (1), and subtitle E of title II of the Homeland Security Act of 2002, based upon the risk of an incident; and

(B) develop guidance that requires agencies to monitor, including automated and continuous monitoring of, the effective implementation of policies, principles, standards, and guidelines developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), paragraph (1), and subtitle E of title II of the Homeland Security Act of 2002;

(C) ensure the effective operation of technical capabilities within the National Center for Cybersecurity and Communications to enable automated and continuous monitoring of any information collected as a result of the guidance developed under subparagraph (B) and use the information to enhance the risk-based security of the Federal information infrastructure; and

(D) ensure the effective operation of a secure system that satisfies information reporting requirements under sections 3553(c) and 3556(c);

(4) require agencies, consistent with the standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) or paragraph (1) and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk resulting from the disruption or unauthorized access, use, disclosure, modification, or destruction of—

(A) information collected or maintained by or on behalf of an agency; or

(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

(5) oversee agency compliance with the requirements of this subchapter, including coordinating with the Office of Management and Budget to use any authorized action under section

11303 of title 40 to enforce accountability for compliance with such requirements;

(6) review, at least annually, and approve or disapprove, agency information security programs required under section 3553(b); and

(7) coordinate information security policies and procedures with the Administrator for Electronic Government and the Administrator for the Office of Information and Regulatory Affairs with related information resources management policies and procedures.

(b) NATIONAL SECURITY SYSTEMS.—The authorities of the Director under this section shall not apply to national security systems.

SEC. 3553. AGENCY RESPONSIBILITIES.

(a) IN GENERAL.—The head of each agency shall—

(1) be responsible for—

(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

(i) information collected or maintained by or on behalf of the agency; and

(ii) agency information infrastructure;

(B) complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including—

(i) information security requirements, including security controls, developed by the Director of the National Center for Cybersecurity and Communications under section 3552, subtitle E of title II of the Homeland Security Act of 2002, or any other provision of law;

(ii) information security policies, principles, standards, and guidelines promulgated under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) and section 3552(a)(1);

(iii) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and

(iv) ensuring the standards implemented for information systems and national security systems of the agency are complementary and uniform, to the extent practicable;

(C) ensuring that information security management processes are integrated with agency strategic and operational planning processes, including policies, procedures, and practices described in subsection (c)(1)(C);

(D) as appropriate, maintaining secure facilities that have the capability of accessing, sending, receiving, and storing classified information;

(E) maintaining a sufficient number of personnel with security clearances, at the appropriate levels, to access, send, receive and analyze classified information to carry out the responsibilities of this subchapter; and

(F) ensuring that information security performance indicators and measures are included in the annual perform-

ance evaluations of all managers, senior managers, senior executive service personnel, and political appointees;

(2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under the control of those officials, including through—

(A) assessing the risk and magnitude of the harm that could result from the disruption or unauthorized access, use, disclosure, modification, or destruction of such information or information systems;

(B) determining the levels of information security appropriate to protect such information and information systems in accordance with policies, principles, standards, and guidelines promulgated under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), section 3552(a)(1), and subtitle E of title II of the Homeland Security Act of 2002, for information security categorizations and related requirements;

(C) implementing policies and procedures to cost effectively reduce risks to an acceptable level;

(D) periodically testing and evaluating information security controls and techniques to ensure that such controls and techniques are operating effectively; and

(E) withholding all bonus and cash awards to senior agency officials accountable for the operation of such agency information infrastructure that are recognized by the Chief Information Security Officer as impairing the risk-based security information, information system, or agency information infrastructure;

(3) delegate to a senior agency officer designated as the Chief Information Security Officer the authority and budget necessary to ensure and enforce compliance with the requirements imposed on the agency under this subchapter, subtitle E of title II of the Homeland Security Act of 2002, or any other provision of law, including—

(A) overseeing the establishment, maintenance, and management of a security operations center that has technical capabilities that can, through automated and continuous monitoring—

(i) detect, report, respond to, contain, remediate, and mitigate incidents that impair risk-based security of the information, information systems, and agency information infrastructure, in accordance with policy provided by the National Center for Cybersecurity and Communications;

(ii) monitor and, on a risk-based basis, mitigate and remediate the vulnerabilities of every information system within the agency information infrastructure;

(iii) continually evaluate risks posed to information collected or maintained by or on behalf of the agency and information systems and hold senior agency officials accountable for ensuring the risk-based security of such information and information systems;

(iv) collaborate with the National Center for Cybersecurity and Communications and appropriate public

and private sector security operations centers to address incidents that impact the security of information and information systems that extend beyond the control of the agency; and

(v) report any incident described under clauses (i) and (ii), as directed by the policy of the National Center for Cybersecurity and Communications or the Inspector General of the agency;

(B) collaborating with the Administrator for E-Government and the Chief Information Officer to establish, maintain, and update an enterprise network, system, storage, and security architecture, that can be accessed by the National Cybersecurity Communications Center and includes—

(i) information on how security controls are implemented throughout the agency information infrastructure; and

(ii) information on how the controls described under subparagraph (A) maintain the appropriate level of confidentiality, integrity, and availability of information and information systems based on—

(I) the policy of the National Center for Cybersecurity and Communications; and

(II) the standards or guidance developed by the National Institute of Standards and Technology;

(C) developing, maintaining, and overseeing an agency-wide information security program as required by subsection (b);

(D) developing, maintaining, and overseeing information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3552;

(E) training, consistent with the requirements of section 406 of the Protecting Cyberspace as a National Asset Act of 2010, and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

(F) assisting senior agency officers concerning their responsibilities under paragraph (2);

(4) ensure that the Chief Information Security Officer has a sufficient number of cleared and trained personnel with technical skills identified by the National Center for Cybersecurity and Communications as critical to maintaining the risk-based security of agency information infrastructure as required by the subchapter and other applicable laws;

(5) ensure that the agency Chief Information Security Officer, in coordination with appropriate senior agency officials, reports not less than annually to the head of the agency on the effectiveness of the agency information security program, including progress of remedial actions;

(6) ensure that the Chief Information Security Officer—

(A) possesses necessary qualifications, including education, professional certifications, training, experience, and the security clearance required to administer the functions described under this subchapter; and

(B) has information security duties as the primary duty of that officer; and

(7) ensure that components of that agency establish and maintain an automated reporting mechanism that allows the Chief Information Security Officer with responsibility for the entire agency, and all components thereof, to implement, monitor, and hold senior agency officers accountable for the implementation of appropriate security policies, procedures, and controls of agency components.

(b) AGENCY-WIDE INFORMATION SECURITY PROGRAM.—Each agency shall develop, document, and implement an agency-wide information security program, approved by the National Center for Cybersecurity and Communications under section 3552(a)(6) and consistent with components across and within agencies, to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes—

(1) frequent assessments, at least twice each month—

(A) of the risk and magnitude of the harm that could result from the disruption or unauthorized access, use, disclosure, modification, or destruction of information and information systems that support the operations and assets of the agency; and

(B) that assess whether information or information systems should be removed or migrated to more secure networks or standards and make recommendations to the head of the agency and the Director of the National Center for Cybersecurity and Communications based on that assessment;

(2) consistent with guidance developed under section 3554, vulnerability assessments and penetration tests commensurate with the risk posed to an agency information infrastructure;

(3) ensure that information security vulnerabilities are remediated or mitigated based on the risk posed to the agency;

(4) policies and procedures that—

(A) are informed and revised by the assessments required under paragraphs (1) and (2);

(B) cost effectively reduce information security risks to an acceptable level;

(C) ensure that information security is addressed throughout the life cycle of each agency information system; and

(D) ensure compliance with—

(i) the requirements of this subchapter;

(ii) policies and procedures prescribed by the National Center for Cybersecurity and Communications;

(iii) minimally acceptable system configuration requirements, as determined by the National Center for Cybersecurity and Communications; and

(iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;

(5) subordinate plans for providing risk-based information security for networks, facilities, and systems or groups of information systems, as appropriate;

(6) role-based security awareness training, consistent with the requirements of section 406 of the Protecting Cyberspace as a National Asset Act of 2010, to inform personnel with access to the agency network, including contractors and other users of information systems that support the operations and assets of the agency, of—

(A) information security risks associated with agency activities; and

(B) agency responsibilities in complying with agency policies and procedures designed to reduce those risks;

(7) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a rigor and frequency depending on risk, which shall include—

(A) testing and evaluation not less than twice each year of security controls of information collected or maintained by or on behalf of the agency and every information system identified in the inventory required under section 3505(c);

(B) the effectiveness of ongoing monitoring, including automated and continuous monitoring, vulnerability scanning, and intrusion detection and prevention of incidents posed to the risk-based security of information and information systems as required under subsection (a)(3); and

(C) testing relied on in—

(i) an operational evaluation under section 3554;

(ii) an independent assessment under section 3556; or

(iii) another evaluation, to the extent specified by the Director;

(8) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

(9) procedures for detecting, reporting, and responding to incidents, consistent with requirements issued under section 3552, that include—

(A) to the extent practicable, automated and continuous monitoring of the use of information and information systems;

(B) requirements for mitigating risks and remediating vulnerabilities associated with such incidents systemically within the agency information infrastructure before substantial damage is done; and

(C) notifying and coordinating with the National Center for Cybersecurity and Communications, as required by this subchapter, subtitle E of title II of the Homeland Security Act of 2002, and any other provision of law; and

(10) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

(c) AGENCY REPORTING.—

(1) IN GENERAL.—Each agency shall.—

(A) ensure that information relating to the adequacy and effectiveness of information security policies, procedures, and practices, is available to the entities identified under paragraph (2) through the system developed under section 3552(a)(3), including information relating to—

(i) compliance with the requirements of this subchapter;

(ii) the effectiveness of the information security policies, procedures, and practices of the agency based on a determination of the aggregate effect of identified deficiencies and vulnerabilities;

(iii) an identification and analysis of any significant deficiencies identified in such policies, procedures, and practices;

(iv) an identification of any vulnerability that could impair the risk-based security of the agency information infrastructure; and

(v) results of any operational evaluation conducted under section 3554 and plans of action to address the deficiencies and vulnerabilities identified as a result of such operational evaluation;

(B) follow the policy, guidance, and standards of the National Center for Cybersecurity and Communications, in consultation with the Federal Information Security Taskforce, to continually update, and ensure the electronic availability of both a classified and unclassified version of the information required under subparagraph (A);

(C) ensure the information under subparagraph (A) addresses the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to—

(i) annual agency budgets;

(ii) information resources management of this subchapter;

(iii) information technology management and procurement under this chapter or any other applicable provision of law;

(iv) subtitle E of title II of the Homeland Security Act of 2002;

(v) program performance under sections 1105 and 1115 through 1119 of title 31, and sections 2801 and 2805 of title 39;

(vi) financial management under chapter 9 of title 31, and the Chief Financial Officers Act of 1990 (31 U.S.C. 501 note; Public Law 101–576) (and the amendments made by that Act);

(vii) financial management systems under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note);

(viii) internal accounting and administrative controls under section 3512 of title 31; and

(ix) performance ratings, salaries, and bonuses provided to the senior managers and supporting personnel taking into account program performance as it relates to complying with this subchapter; and

(D) report any significant deficiency in a policy, procedure, or practice identified under subparagraph (A) or (B)—

(i) as a material weakness in reporting under section 3512 of title 31; and

(ii) if relating to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note).

(2) ADEQUACY AND EFFECTIVENESS INFORMATION.—Information required under paragraph (1)(A) shall, to the extent possible and in accordance with applicable law, policy, guidance, and standards, be available on an automated and continuous basis to—

(A) the National Center for Cybersecurity and Communications;

(B) the Committee on Homeland Security and Governmental Affairs of the Senate;

(C) the Committee on Government Oversight and Reform of the House of Representatives;

(D) the Committee on Homeland Security of the House of Representatives;

(E) other appropriate authorization and appropriations committees of Congress;

(F) the Inspector General of the Federal agency; and

(G) the Comptroller General.

(d) INCLUSIONS IN PERFORMANCE PLANS.—

(1) IN GENERAL.—In addition to the requirements of subsection (c), each agency, in consultation with the National Center for Cybersecurity and Communications, shall include as part of the performance plan required under section 1115 of title 31 a description of the time periods the resources, including budget, staffing, and training, that are necessary to implement the program required under subsection (b).

(2) RISK ASSESSMENTS.—The description under paragraph (1) shall be based on the risk and vulnerability assessments required under subsection (b) and evaluations required under section 3554.

(e) NOTICE AND COMMENT.—Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.

(f) MORE STRINGENT STANDARDS.—The head of an 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 the Director of the National Center for Cybersecurity and Communications prescribes under this subchapter, subtitle E of title II of the Homeland Security Act of 2002, or any other provision of law, if the more stringent standards—

(1) contain at least the applicable standards made compulsory and binding by the Director of the National Center for Cybersecurity and Communications; and

(2) are otherwise consistent with policies and guidelines issued under section 3552.

SEC. 3554. ANNUAL OPERATIONAL EVALUATION.

(a) GUIDANCE.—

(1) IN GENERAL.—Each year the National Center for Cybersecurity and Communications shall oversee, coordinate, and develop guidance for the effective implementation of operational evaluations of the Federal information infrastructure and agency information security programs and practices to determine the effectiveness of such program and practices.

(2) COLLABORATION IN DEVELOPMENT.—In developing guidance for the operational evaluations described under this section, the National Center for Cybersecurity and Communications shall collaborate with the Federal Information Security Taskforce and the Council of Inspectors General on Integrity and Efficiency, and other agencies as necessary, to develop and update risk-based performance indicators and measures that assess the adequacy and effectiveness of information security of an agency and the Federal information infrastructure.

(3) CONTENTS OF OPERATIONAL EVALUATION.—Each operational evaluation under this section—

(A) shall be prioritized based on risk; and

(B) shall—

(i) test the effectiveness of agency information security policies, procedures, and practices of the information systems of the agency, or a representative subset of those information systems;

(ii) assess (based on the results of the testing) compliance with—

(I) the requirements of this subchapter; and

(II) related information security policies, procedures, standards, and guidelines;

(iii) evaluate whether agencies—

(I) effectively monitor, detect, analyze, protect, report, and respond to vulnerabilities and incidents;

(II) report to and collaborate with the appropriate public and private security operation centers, the National Center for Cybersecurity and Communications, and law enforcement agencies; and

(III) remediate or mitigate the risk posed by attacks and exploitations in a timely fashion in order to prevent future vulnerabilities and incidents; and

(iv) identify deficiencies of agency information security policies, procedures, and controls on the agency information infrastructure.

(b) CONDUCT AN OPERATIONAL EVALUATION.—

(1) IN GENERAL.—Except as provided under paragraph (2), and in consultation with the Chief Information Officer and senior officials responsible for the affected systems, the Chief Information Security Officer of each agency shall not less than annually—

(A) conduct an operational evaluation of the agency information infrastructure for vulnerabilities, attacks, and exploitations of the agency information infrastructure;

(B) evaluate the ability of the agency to monitor, detect, correlate, analyze, report, and respond to incidents; and

(C) report to the head of the agency, the National Center for Cybersecurity and Communications, the Chief Information Officer, and the Inspector General for the agency the findings of the operational evaluation.

(2) SATISFACTION OF REQUIREMENTS BY OTHER EVALUATION.—Unless otherwise specified by the Director of the National Center for Cybersecurity and Communications, if the National Center for Cybersecurity and Communications conducts an operational evaluation of the agency information infrastructure under section 245(b)(2)(A) of the Homeland Security Act of 2002, the Chief Information Security Officer may deem the requirements of paragraph (1) satisfied for the year in which the operational evaluation described under this paragraph is conducted.

(c) CORRECTIVE MEASURES MITIGATION AND REMEDIATION PLANS.—

(1) IN GENERAL.—In consultation with the National Center for Cybersecurity and Communications and the Chief Information Officer, Chief Information Security Officers shall remediate or mitigate vulnerabilities in accordance with this subsection.

(2) RISK-BASED PLAN.—After an operational evaluation is conducted under this section or under section 245(b) of the Homeland Security Act of 2002, the agency shall submit to the National Center for Cybersecurity and Communications in a timely fashion a risk-based plan for addressing recommendations and mitigating and remediating vulnerabilities identified as a result of such operational evaluation, including a timeline and budget for implementing such plan.

(3) APPROVAL OR DISAPPROVAL.—Not later than 15 days after receiving a plan submitted under paragraph (2), the National Center for Cybersecurity and Communications shall—

(A) approve or disapprove the agency plan; and

(B) comment on the adequacy and effectiveness of the plan.

(4) ISOLATION FROM INFRASTRUCTURE.—

(A) IN GENERAL.—The Director of the National Center for Cybersecurity and Communications may, consistent with the contingency or continuity of operation plans applicable to such agency information infrastructure, order the isolation of any component of the Federal information infrastructure from any other Federal information infrastructure, if—

(i) an agency does not implement measures in a risk-based plan approved under this subsection; and

(ii) the failure to comply presents a significant danger to the Federal information infrastructure.

(B) DURATION.—An isolation under subparagraph (A) shall remain in effect until—

(i) the Director of the National Center for Cybersecurity and Communications determines that corrective measures have been implemented; or

(ii) an updated risk-based plan is approved by the National Center for Cybersecurity and Communications and implemented by the agency.

(d) OPERATIONAL GUIDANCE.—The Director of the National Center for Cybersecurity and Communications shall—

(1) not later than 180 days after the date of enactment of the Protecting Cyberspace as a National Asset Act of 2010, develop operational guidance for operational evaluations as required under this section that are risk-based and cost effective; and

(2) periodically evaluate and ensure information is available on an automated and continuous basis through the system required under section 3552(a)(3)(D) to Congress on—

(A) the adequacy and effectiveness of the operational evaluations conducted under this section or section 245(b) of the Homeland Security Act of 2002; and

(B) possible executive and legislative actions for cost-effectively managing the risks to the Federal information infrastructure.

SEC. 3555. FEDERAL INFORMATION SECURITY TASKFORCE.

(a) ESTABLISHMENT.—There is established in the executive branch a Federal Information Security Taskforce.

(b) MEMBERSHIP.—The members of the Federal Information Security Taskforce shall be full-time senior Government employees and shall be as follows:

(1) The Director of the National Center for Cybersecurity and Communications.

(2) The Administrator of the Office of Electronic Government of the Office of Management and Budget.

(3) The Chief Information Security Officer of each agency described under section 901(b) of title 31.

(4) The Chief Information Security Officer of the Department of the Army, the Department of the Navy, and the Department of the Air Force.

(5) A representative from the Office of Cyberspace Policy.

(6) A representative from the Office of the Director of National Intelligence.

(7) A representative from the United States Cyber Command.

(8) A representative from the National Security Agency.

(9) A representative from the United States Computer Emergency Readiness Team.

(10) A representative from the Intelligence Community Incident Response Center.

(11) A representative from the Committee on National Security Systems.

(12) A representative from the National Institute for Standards and Technology.

(13) A representative from the Council of Inspectors General on Integrity and Efficiency.

(14) A representative from State and local government.

(15) Any other officer or employee of the United States designated by the chairperson.

(c) CHAIRPERSON AND VICE-CHAIRPERSON.—

(1) CHAIRPERSON.—The Director of the National Center for Cybersecurity and Communications shall act as chairperson of the Federal Information Security Taskforce.

(2) VICE-CHAIRPERSON.—The vice chairperson of the Federal Information Security Taskforce shall—

(A) be selected by the Federal Information Security Taskforce from among its members;

(B) serve a 1-year term and may serve multiple terms; and

(C) serve as a liaison to the Chief Information Officer, Council of the Inspectors General on Integrity and Efficiency, Committee on National Security Systems, and other councils or committees as appointed by the chairperson.

(d) FUNCTIONS.—The Federal Information Security Taskforce shall—

(1) be the principal interagency forum for collaboration regarding best practices and recommendations for agency information security and the security of the Federal information infrastructure;

(2) assist in the development of and annually evaluate guidance to fulfill the requirements under sections 3554 and 3556;

(3) share experiences and innovative approaches relating to threats against the Federal information infrastructure, information sharing and information security best practices, penetration testing regimes, and incident response, mitigation, and remediation;

(4) promote the development and use of standard performance indicators and measures for agency information security that—

(A) are outcome-based;

(B) focus on risk management;

(C) align with the business and program goals of the agency;

(D) measure improvements in the agency security posture over time; and

(E) reduce burdensome and efficient performance indicators and measures;

(5) recommend to the Office of Personnel Management the necessary qualifications to be established for Chief Information Security Officers to be capable of administering the functions described under this subchapter including education, training, and experience;

(6) enhance information system processes by establishing a prioritized baseline of information security measures and controls that can be continuously monitored through automated mechanisms;

(7) evaluate the effectiveness and efficiency of any reporting and compliance requirements that are required by law related to the information security of Federal information infrastructure; and

(8) submit proposed enhancements developed under paragraphs (1) through (7) to the Director of the National Center for Cybersecurity and Communications.

(e) TERMINATION.—

(1) IN GENERAL.—Except as provided under paragraph (2), the Federal Information Security Taskforce shall terminate 4 years after the date of enactment of the Protecting Cyberspace as a National Asset Act of 2010.

(2) EXTENSION.—The President may—

(A) extend the Federal Information Security Taskforce by executive order; and

(B) make more than 1 extension under this paragraph for any period as the President may determine.

SEC. 3556. INDEPENDENT ASSESSMENTS.

(a) IN GENERAL.—

(1) INSPECTORS GENERAL ASSESSMENTS.—Not less than every 2 years, each agency with an Inspector General appointed under the Inspector General Act of 1978 (5 U.S.C. App.) shall assess the adequacy and effectiveness of the information security program developed under section 3553(b) and (c), and evaluations conducted under section 3554.

(2) INDEPENDENT ASSESSMENTS.—For each agency to which paragraph (1) does not apply, the head of the agency shall engage an independent external auditor to perform the assessment.

(b) EXISTING ASSESSMENTS.—The assessments required by this section may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

(c) INSPECTORS GENERAL REPORTING.—Inspectors General shall ensure information obtained as a result of the assessment required under this section, or any other relevant information, is available through the system required under section 3552(a)(3)(D) to Congress and the National Center for Cybersecurity and Communications.

SEC. 3557. PROTECTION OF INFORMATION.

In complying with this subchapter, agencies, evaluators, and Inspectors General shall take appropriate actions to ensure the protection of information which, if disclosed, may adversely affect information security. Protections under this chapter shall be commensurate with the risk and comply with all applicable laws and regulations.

SEC. 3558. DEPARTMENT OF DEFENSE AND CENTRAL INTELLIGENCE AGENCY SYSTEMS.

(a) IN GENERAL.—The authorities of the Director of the National Center for Cybersecurity and Communications under this subchapter shall be delegated to—

(1) the Secretary of Defense in the case of systems described under subsection (b)

(2) the Director of Central Intelligence in the case of systems described in subsection (c).

(b) DEPARTMENT OF DEFENSE SYSTEMS.—The systems described in this paragraph are systems that are operated by the Department of Defense, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Department of Defense.

(c) CENTRAL INTELLIGENCE AGENCY SYSTEMS.—The systems described in this paragraph are systems that are operated by the Central Intelligence Agency, a contractor of the Central Intelligence Agency, or another entity on behalf of the Central Intelligence Agency that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would

have a debilitating impact on the mission of the Central Intelligence Agency.

○