Calendar No. 564

113TH CONGRESS *2d Session*	SENATE	REPORT 113–256

FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 2521

TO AMEND CHAPTER 35 OF TITLE 44, UNITED STATES CODE, TO PROVIDE FOR REFORM TO FEDERAL INFORMATION SECURITY

SEPTEMBER 15, 2014.—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE

39–010 WASHINGTON : 2014

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

THOMAS R. CARPER, Delaware *Chairman*

CARL LEVIN, Michigan
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
CLAIRE MCCASKILL, Missouri
JON TESTER, Montana
MARK BEGICH, Alaska
TAMMY BALDWIN, Wisconsin
HEIDI HEITKAMP, North Dakota

TOM COBURN, Oklahoma
JOHN MCCAIN, Arizona
RON JOHNSON, Wisconsin
ROB PORTMAN, Ohio
RAND PAUL, Kentucky
MICHAEL B. ENZI, Wyoming
KELLY AYOTTE, New Hampshire

GABRIELLE A. BATKIN, *Staff Director*
JOHN P. KILVINGTON, *Deputy Staff Director*
MARY BETH SCHULTZ, *Chief Counsel*
STEPHEN R. VIÑA, *Chief Counsel for Homeland Security*
MATTHEW R. GROTE, *Senior Professional Staff Member*
KEITH B. ASHDOWN, *Minority Staff Director*
CHRISTOPHER J. BARKLEY, *Minority Deputy Staff Director*
ANDREW C. DOCKHAM, *Minority Chief Counsel*
DANIEL P. LIPS, *Minority Director of Homeland Security*
JUSTIN ROOD, *Minority Director of Investigations*
WILLIAM H.W. MCKENNA, *Minority Investigative Counsel*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 564

113TH CONGRESS, 2d Session | SENATE | REPORT 113–256

FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014

SEPTEMBER 15, 2014.—Ordered to be printed

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

R E P O R T

[To accompany S. 2521]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 2521), to amend chapter 35 of title 44, United States Code, to provide for reform to Federal information security, having considered the same, reports favorably thereon without amendment and recommends that the bill do pass.

CONTENTS

I. PURPOSE AND SUMMARY

S. 2521, the Federal Information Security Modernization Act, aims to strengthen the security of federal computer networks and information systems by updating the Federal Information Security Management Act of 2002. Specifically, it would: (1) clarify the roles and responsibilities of the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) to ensure that the statute appropriately reflects each agency's current functions, as well as their respective expertise and resources; (2) improve security by transitioning agencies away from paperwork requirements toward a more automated and continuous security posture; and (3) strengthen transparency and accountability including

by making important improvements to the way federal data breaches are managed and reported to Congress and the public.

II. Background and the Need for Legislation

In 2002, President Bush signed into law the Federal Information Security Management Act of 2002 (FISMA), which built on existing information security laws,[1] to "provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets."[2] This law aimed to protect all information and information systems held by or on behalf of Federal agencies from unauthorized access, use, disclosure, disruption, modification, or destruction. Under FISMA, a number of different federal agencies play a variety of roles in implementing the law's framework. For example, the National Institute of Standards and Technology (NIST) develops minimum security standards for federal information and information systems (other than national security systems).[3] Agencies, through the Chief Information Officers and system owners, were required to establish information security programs with specific elements, implement minimum system security standards, and report to OMB and Congress on implementation progress. FISMA gave OMB the role of overseeing and enforcing agency compliance with the law and security standards. Finally, the bill required Inspectors General to audit agencies' compliance with the law annually, and Government Accountability Office to periodically review the effectiveness of the overall framework.

Since the passage of FISMA, agencies have made progress in setting up consistent information security programs across government. Unfortunately, however, they have not kept up with the cyber threat that has grown even faster and larger than Congress could have foreseen in 2002. Over the past two decades, the growth of the Internet and the country's increasing use of interconnected networks to conduct its business has led to significant economic growth and innovation. However, this ever-increasing reliance upon the Internet has also unintentionally enabled new threats to develop. Indeed, the Federal Bureau of Investigation Director James Comey testified before the Homeland Security and Governmental Affairs Committee that he agreed with former-Director Robert Mueller's assessment that within the next ten years cyber threats would surpass the threat from foreign terrorists to the United States.[4]

Criminals, terrorists, and state actors have repeatedly shown their interest in attacking the computer networks that run so much of our economy, and have made clear that government systems are also in their sights.[5] For example, in 2011, the Thrift Savings Plan

---

[1] For example, the Computer Security Act of 1987 established government-wide mandatory standards for computer security developed by the National Institute of Standards and Technology (NIST) and required certain security plans and training; see Public Law No. 100–235 (H.R. 145), (Jan. 8, 1988).

[2] *See* 44 USC § 35; 44 section § 3541.

[3] NIST received this charge in the Computer Security Act of 1987; See Public Law No. 100–235 (H.R. 145), (Jan. 8, 1988).

[4] *See* "Threats to the Homeland" hearing, Committee on Homeland Security and Governmental Affairs, U.S. Senate, November 14, 2013.

[5] Some actors in cyberspace also seek to disrupt or destroy computer systems, including those that control some of our nation's critical infrastructure—the systems that deliver power and water to our homes, our energy pipelines, our nuclear plants and our telecommunications sys-

(TSP), the retirement savings and investment plan used by millions of federal employees and members of the uniformed services, suffered a data security breach, allowing unauthorized access to the personal information of approximately 123,000 TSP participants.[6] And, in 2013, malicious actors broke into the computer network at the Department of Energy's Washington headquarters and compromised the personal information of hundreds of employees.[7] The Government Accountability Office has written that from 2006 to 2012, "the number of incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team[8] (US–CERT) has increased from 5,503 in fiscal year 2006 to 48,562 incidents in fiscal year 2012, an increase of 782 percent."[9]

Given the ever-increasing threat, the Committee believes that Congress must do everything possible to make government computer networks as strong as possible. S. 2521 would do that by modernizing and strengthening the current, outdated statutory framework governing federal information security. Specifically, it would: clarify the roles of the OMB and DHS; reduce paperwork and speed up the move toward real-time security; and make important improvements to the way federal data breaches are handled.

CODIFYING AND CLARIFYING THE ROLES OF OMB AND DHS

S. 2521 updates FISMA to codify and clarify the existing roles that DHS and OMB play in overseeing and securing federal agency computer networks. Under FISMA, the Director of OMB has exclusive authority to oversee the management and security of information security across federal civilian agencies. These functions include developing and overseeing information security policies, principles, standards and guidelines, requiring agencies to identify and provide information security protections commensurate with risk, and overseeing agency compliance with the requirements of FISMA, among other things. Although DHS does not have an explicit statutory role under FISMA, the Department currently performs a variety of functions, including providing cybersecurity services for federal civilian agencies across the government, under a patchwork of other authorities.

---

tems. In Saudi Arabia, for example, a cyber attack against Saudi Aramco, one of the world's largest oil companies, damaged 30,000 computers on the company's network. *See Worldwide Threat Assessment of the US Intelligence Community,* Hearing before the House Permanent Select Committee on Intelligence, Written Statement of James R. Clapper, Director of National Intelligence (April 11, 2013). To date, there has been no similarly damaging cyber attack with physical effects to critical infrastructure in the United States. However, in 2013, major financial institutions were targeted by repeated "denial-of-service" cyber attacks, which attempted to disrupt the performance of company websites by flooding them with internet traffic. *Id.*

[6] *See* Federal Retirement Thrift Investment Board, Press Release, "Federal Retirement Thrift Investment Board Reports a Cyber Attack on a Contractor Potentially Affecting TSP Participants" (May 25, 2012) https://www.tsp.gov/PDF/formspubs/Press.Release.2012–05–25.Cyber.pdf (last accessed July 20, 2014).

[7] *See* Department of Energy, Office of the Inspector General, The Department of Energy's July 2013 Cyber Security Breach, DOE/IG–0900 (Washington, D.C.: Dec. 6, 2013) http://energy.gov/sites/prod/files/2013/12/f5/IG–0900.pdf (last accessed July 20, 2014).

[8] US–CERT within DHS provides technical and incident response assistance to operators of agency information systems.

[9] *See* GAO–13–776, "Federal Information Security: Mixed Progress In Implementing Program Components; Improved Metrics Needed To Measure Effectiveness," pages 8, 27, September 26, 2013. It is likely that some of these increases can be attributed to better reporting tools and metrics. For example, the increased use of automated discovery and monitoring tools has uncovered more security flaws than were known in past years and it is the hope that more visibility will bring more attention to prevent these vulnerabilities. Nonetheless, critical weaknesses continue to exist in agencies' security programs.

In January 2008, President Bush issued National Security Presidential Directive 54/Homeland Security Presidential Directive 23, which, among other things, required DHS to lead the national effort to secure Federal networks and to coordinate and carry out government-wide security programs. The directive required DHS to "lead the national effort to protect, defend, and reduce vulnerabilities of Federal systems," including to "manage and oversee . . . the external access points, including access to the Internet for all Federal systems," "provide consolidated intrusion detection, incident analysis, and cyber response capabilities," and set and enforce minimum operational standards for agency operation centers to manage external access points.[10]

In 2010, OMB issued M–10–28, "Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security". This memorandum delegated most of OMB's FISMA oversight functions to DHS and stated that "DHS will exercise primary responsibility within the executive branch for the operational aspects of Federal agency cybersecurity." [11] Specifically, the memo made DHS responsible for:

- overseeing the government-wide and agency-specific implementation of and reporting on cybersecurity policies and guidance;
- overseeing and assisting government-wide and agency-specific efforts to provide adequate, risk-based and cost-effective cybersecurity;
- overseeing the agencies' compliance with FISMA and developing analyses for OMB to assist in the development of the FISMA annual report;
- overseeing the agencies' cybersecurity operations and incident response and providing appropriate assistance; and
- annually reviewing the agencies' cybersecurity programs.[12]

Under this memorandum, OMB submits the annual implementation report to Congress required by FISMA and carries out its traditional budgetary and fiscal oversight responsibilities with respect to agency spending on information security. OMB also oversees DHS in implementing its responsibilities under the memorandum. OMB's delegation of certain FISMA responsibilities to DHS is a sound move that has been and will continue to improve our federal information security.

Within the federal government, DHS is responsible for working with the private sector to help protect our Nation's critical infrastructure from physical and cyber threats and overseeing the protection of the .gov domain. DHS employs over 400 personnel dedicated to the security of government networks, and in fiscal year 2014 DHS was appropriated $680 million for its efforts on federal network security, network security deployment, and the United States Computer Emergency Readiness Team (US–CERT).[13] OMB, on the other hand, has the equivalent of only 2–3 full-time employ-

---

[10] *See* National Security Presidential Directive 54/Homeland Security Presidential Directive 23 "Cybersecurity Policy", paragraph 15, January 8, 2008.

[11] *See* Office of Management and Budget, Memorandum M–10–28, "Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security" (July 6, 2010).

[12] *Id.*

[13] *See* Department of Homeland Security, Congressional Budget Justification Fiscal Year 2015, page 9 (February 2014).

ees on the "management" side overseeing security for the entire federal government and does not possess the technical capabilities of an operational department such as DHS.

At the center of DHS' cybersecurity and communications mission is the National Cybersecurity and Communications Integration Center (NCCIC). The NCICC is a round-the-clock information sharing, analysis and incident response center where government, private sector, and international partners work together on cybersecurity matters. Among its various functions, the NCCIC: analyzes cybersecurity and communications threats and vulnerabilities and coordinates findings with partners to manage risks to critical systems; creates shared situational awareness among public sector, private sector, and international partners by collaboratively developing and sharing timely and actionable cybersecurity and communications information; and responds cybersecurity and communications incidents and events to mitigate harmful activity, manage crisis situations, and support recovery efforts.

Operation of the NCCIC gives DHS the ability to see and understand cyber threats and to find ways to mitigate against such threats, risks, and vulnerabilities. This insight is an extremely valuable tool, one that helps DHS to assist federal agencies in effectively implementing federal information security measures. In fiscal year 2013 alone, the NCCIC responded to more than 228,000 incident reports from a variety of stakeholders, ranging from minor compromises of personal information up to mass data thefts. The NCCIC also released over 11,000 cyber alerts to industry, federal agencies, and other partners in fiscal year 2013 and more than 5,000 organizations have used the NCCIC's tools to perform self-assessments to identify their own vulnerabilities.[14]

Since memoranda M–10–28 was issued, DHS has taken on the role of operational oversight of FISMA implementation and assisted agencies in bolstering their security. For example, DHS's National Protection and Programs Directorate (NPPD) has overseen government-wide FISMA compliance by issuing several policy directives, collecting and analyzing monthly compliance data, working with senior management at agencies to increase compliance, and updating reporting metrics to be more performance-based. DHS has also taken several measures to improve its own network security and scored first in its FISMA compliance among all major agencies in 2013.[15]

As mentioned above, OMB's delegation of many of its FISMA responsibilities was done through a memorandum. There has been no explicit statutory grant of authority of DHS's FISMA responsibilities. This lack of statutory clarity has led to uncertainty regarding the roles of DHS and OMB, resulting in inefficiencies and confusion. For example, in 2013, OMB and DHS released conflicting guidance to agencies on the same topic, annual reporting instruc-

[14] Department of Homeland Security, NCCIC Weekly Cyber Analytics Report, Week ending 14 June 2014 (on file with Committee staff).

[15] *See* "Annual Report to Congress: Federal Information Security Management Act", OMB, May 1, 2014, page 61. In 2012, DHS tied for first place with two other agencies. See "Fiscal Year 2012 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002", OMB, March 2013, page 41.

tions to agencies on security implementation.[16] A recent GAO report recognized the problems caused by the confusion regarding the roles and responsibilities of DHS and OMB, and GAO recommended that Congress consider passing legislation to clarify the respective agencies roles and responsibilities regarding implementation of and oversight of federal information security.[17]

The Committee agrees that having clear statutory roles and responsibilities is beneficial in this area. This bill would address these concerns by codifying and clarifying the existing roles and responsibilities of DHS and OMB as described in memorandum M–10–28. Under this bill, OMB would retain federal information security enforcement responsibilities through its budget powers and its discretion in setting over-arching information security policies. DHS would continue to carry out the responsibilities delegated to it under the memorandum to oversee operational aspects of agency information security policies and practices, including by developing and overseeing implementation of binding operational directives to federal agencies, setting requirements for reporting security incidents and requirements for annual reports, establishing requirements for the mitigation of exigent risks, collecting implementation data, convening meetings with agencies to help ensure effective implementation of federal information security, coordinating government-wide information security efforts, and providing operational and technical assistance to agencies on information security. This structure is similar to the way other agencies share government-wide policy and implementation responsibilities in highly-technical areas. For example, the General Services Administration sets property management regulations that agencies must carry out and the Office of Personnel Management sets standards for personnel management that agencies must carry out.[18]

Under the bill, DHS would also assist agencies in implementing information security programs, including by operating the Federal information security incident center, deploying continuous diagnostics and mitigation capabilities, compiling and analyzing data on agency information security, and conducting targeted operational evaluations.

CONTINUOUS MONITORING

Over the years a number of experts have called for reform of the Federal information security framework to move away from paperwork-heavy processes toward real-time and automated security. Continuous monitoring, for example, allows federal agencies to monitor the effectiveness of security controls with a frequency based on risk and often in an automated fashion using security tools. It is common practice for a system owner to "authorize" that a system has adequate security before a system is active for the first time or if it undergoes a major change. Within the Federal government, this process is traditionally known as "Certification and Accreditation," and agencies have been required to produce large binders of paperwork every three years to assure that adequate security controls were in place. This process has been criti-

[16] *See* GAO–13–187, "Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented", February 14, 2013, page 33.
[17] *Id.* at page 83.
[18] *See* 40 U.S.C. § 121(c), and 5 U.S.C. § 1104(b).

cized for requiring vast amounts of paperwork for little return on security.[19] The modern approach to providing assurance of security controls involves automated monitoring and diagnostics with greater frequency and less paperwork.[20]

One of the main obstacles to full adoption of the modern, automated approach is a policy issued in 2000 by the Office of Management and Budget known as Circular A–130 Appendix III. This policy, which originated in the 1980's, has not been revised in over thirteen years despite the ever-changing nature of the cyber threat and information security best practices. It requires agencies to document the implementation of security controls on their systems every three years, which can result in large binders of paperwork. While some level of documentation is necessary to provide assurance of the effectiveness of controls, the requirements in this policy are not cost-effective methods to reduce information security risk. Experts have called for the rewrite of Circular A–130, stating that "absent changes in policy, agency staff and oversight groups (e.g., Inspectors General and the Government Accountability Office) will continue to waste scarce resources on strategies that do little to mitigate risk."[21] S. 2521 would move toward continuous and automated monitoring by requiring the Office of Management and Budget to revise A–130 within 180 days to eliminate these inefficient and wasteful reports.

Another way S. 2521 helps agencies improve security is by codifying the existing Continuous Diagnostics and Mitigation program at DHS. This program offers advanced security technologies to all agencies with the potential advantage of bulk-buying economies.[22] In particular, the program offers software to implement the modern approach of automated security.

STRENGTHENING ACCOUNTABILITY AND TRANSPARENCY THROUGH CYBER INCIDENT NOTIFICATION

Finally, the bill would make important improvements to the way federal data breaches are managed. For example, the bill calls on federal agencies to provide timely notice to victims when their personally identifiable information is stolen from government networks. When it comes to responding to a data breach and notifying the public, it is very important for the federal government to be transparent and lead by example.

Currently, agencies are required by OMB policy to publicly report only security incidents that affect personal information of indi-

---

[19] *See* "More Security, Less Waste: What Makes Sense for our Federal Cyber Defense", Federal Financial Management Subcommittee, Committee on Homeland Security and Governmental Affairs, United States Senate, October 29, 2009. *See* "Updating U.S. Federal Cybersecurity Policy and Guidance," Center for Strategic and International Studies, page 3, October 2012.

[20] *See* "Federal Departments and Agencies Focus Cybersecurity Activity on Three Administration Priorities," Howard Schmidt, Cybersecurity Coordinator and Special Assistant to the President, March 23, 2012; "Continuous Diagnostics and Mitigation," Department of Homeland Security. *See* "Special Publication 800–37, Guide for Applying the Risk Management Framework to Federal Information Systems," National Institute of Standards and Technology, page 1, February 2010. Current law requires agencies to test their systems "with a frequency depending on risk, but no less than annually". *See* 44 U.S.C. 3542(b)(5). This requirement is flexible enough for agencies to adopt continuous monitoring programs prescribed by the National Institute of Standards and Technology.

[21] *See* "Updating U.S. Federal Cybersecurity Policy and Guidance," Center for Strategic and International Studies, page 1, October 2012.

[22] *See* "Continuous Diagnostics and Mitigation," Department of Homeland Security, http://www.dhs.gov/cdm, last accessed July 8, 2014.

viduals, with certain restrictions.[23] Even then, the reports that are made are often inconsistent and don't have to go to Congress. Further, mandated management reports all focus on implementation compliance rather than actual incidents. For example, the annual reports to Congress required by FISMA from every agency are often dozens of pages long and show implementation levels of certain elements of agencies' information security programs. However, these reports provide Congress with only a limited view of how effective the security investments truly are. While it is difficult to measure security, the Committee believes that these reports would provide a clearer picture if they detailed major information security incidents at the agencies. Better transparency on incidents allows for more effective management and oversight of information security programs.

The Government Accountability Office found that agencies' responses to breaches of personally identifiable information were inconsistent, partly due to incomplete guidance from OMB.[24] S. 2521 would require OMB to issue data breach guidance to agencies requiring timely notification of breaches to victims and federal cybersecurity centers. The Director of OMB is required to consider the recommendations of GAO when establishing its policies and procedures for agencies to follow in the event of a breach.

Currently, there are no requirements for all agencies to notify Congress about major information security breaches. Management reports, such as the annual FISMA reports, typically focus on compliance of implementation of program requirements. While full implementation of program requirements is important, compliance data does not provide a complete picture of the effectiveness of security programs. The bill would require that major incidents are reported to Congress and that incidents are included in management and oversight reports.

OTHER AMENDMENTS

Importantly, the bill requires the head of agencies to ensure that all personnel are held accountable for complying with the agency-wide information security program. Information security requires compliance and vigilance from all employees to ensure that there are no unnecessary weaknesses or vulnerabilities in each system. Requiring agencies to hold all employees accountable for complying with information security guidelines is an important measure to strengthen the security of federal networks and information systems.

The bill makes several other minor changes to modernize the law. For example, to strengthen the oversight powers of department-level Chief Information Officers over component and agency information systems, the bill would require that senior agency officials (including component agency Chief Information Officers) carry out the directions of the department-level Chief Information Officer. It would also give Inspectors General more flexibility in how they audit security programs, require the Federal information security incident center at section 3556 of the bill to share threat intel-

[23] *See* OMB M–7–16 "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," May 22, 2007, page 13.

[24] GAO–14–34 "Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent," December 9, 2013, page 26.

ligence with agencies, and require that the existing Information Security and Privacy Advisory Board, which currently advises NIST, also advise DHS.

III. LEGISLATIVE HISTORY

Chairman Carper and Ranking Member Coburn introduced S. 2521 on June 24, 2014. The bill was referred to the Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 2521 at a business meeting on June 25, 2014 and ordered the bill reported favorably by voice vote. Senators present for vote on the bill were Senators Carper, Levin, Pryor, Landrieu, McCaskill, Tester, Heitkamp, Coburn, McCain, Johnson, and Portman.

IV. SECTION-BY-SECTION ANALYSIS OF THE BILL, AS REPORTED

Section 1. Short title

The short title of the bill is the "Federal Information Security Modernization Act of 2014".

Section 2. FISMA reform

Subsection (a)

This subsection amends 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 replacing them with a new subchapter. This new subchapter, however, retains the vast majority of original FISMA requirements. The following section-by-section analysis focuses on how this bill amends the original FISMA language.

New Section 3551. Purposes

Section 3551 maintains the language under current FISMA stating that the purposes of this subchapter are to provide a comprehensive policy and oversight framework for federal agencies' information security.

New Section 3552. Definitions

Section 3552 uses the same definitions that FISMA currently uses for the terms "information security", "information technology", "national security system", and the definitions under section 3502, from which FISMA derives much of its terminology. This section adds to the original FISMA language definitions for the terms "binding operational directive", "incident", "intelligence community", and "Secretary". The term "binding operational directive" means a compulsory direction to an agency that is in accordance with policies, principles, standards, and guidelines issued by the Director. The definition for 'incident' is derived from widely used guidance issued by the National Institute of Standards and Technology and the Committee on National Security Systems.

New Section 3553. Authority and functions of the Director and the Secretary

Section 3553 codifies and clarifies the roles currently played by the Director of the Office of Management and Budget (OMB) and

the Secretary of Homeland Security, consistent with OMB Memoranda M–10–28.

The Director would oversee agency information security policies, including developing and overseeing implementation of policies, requiring agencies to provide adequate information security protections, ensuring that the Secretary carries out the authorities and functions that have been assigned to him; coordinating the development of security standards, coordinating information security policy with information technology management policy, and consulting with the Secretary in carrying out OMB's authorities and functions under this subsection. This section maintains the scope of information and information systems subject to the requirements of FISMA set out by current law and OMB guidance.

The Secretary would oversee the operational aspects of information security policies, including assisting the Director in fulfilling OMB's responsibilities under the bill. The Secretary would develop and oversee implementation of binding operational directives in accordance with overarching policies issued by the Director. The Secretary would monitor agency implementation of information security policies and practices, convene oversight meetings with agency officials, coordinate government-wide information security efforts and provide operational and technical assistance to agencies in implementing policies, principles, standards and guidelines on information security.

The Secretary would also assist agencies in implementing information security programs, including by operating the Federal information security incident center, by deploying continuous diagnostics and mitigation capabilities, compiling and analyzing data on agency information security, and conducting targeted operational evaluations.

The section would require the Director, in consultation with the Secretary, to report annually to Congress on the effectiveness of agency implementation of information security programs, including providing a summary of information security incidents across the federal government.

This section would maintain the treatment of national security systems under current law. Current law gives the Secretary of Defense and the Director of National Intelligence policy and oversight authorities for systems critical to their missions.

New Section 3554. Federal agency responsibilities

Section 3554 maintains much of current law that lays out responsibilities of agency heads to provide adequate security for the information and systems under their control. This section clarifies that Department heads would be required to ensure that component chief information officers follow the directions of the department-level chief information officer on information security matters. Agencies would be required to report major information security incidents to Congress, for incidents affecting information collected or maintained by or on behalf of the agency and information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency. Agency heads would report annually on the effectiveness of their security programs, along with a summary of incidents, and identify significant deficiencies and processes to remediate those deficiencies. This sec-

tion maintains the scope of information and information systems subject to the requirements of FISMA set out by current law and OMB guidance, and the responsibilities of agency heads to provide adequate security for those information and information systems. The bill also requires heads of agencies to ensure that all personnel are held accountable for complying with agency-wide information security program requirements.

New Section 3555. Annual independent evaluation

Section 3555 maintains much of current law and gives inspectors general additional flexibility in conducting their annual reviews under current law. GAO would provide technical assistance to inspectors general in conducting security reviews.

New Section 3556. Federal information security incident center

Section 3556 maintains much of current law and requires the federal information security incident center, which is responsible for providing technical and incident response assistance to agencies, to share threat intelligence with agencies.

New Section 3557. National security systems

Section 3557 maintains the language under current law to ensure that agencies provide security for national security systems.

New Section 3558. Effect on existing law

Section 3558 maintains the language under current law to provide that nothing in this subchapter or those provisions of law relating to the development and promulgation of NIST-developed standards may be construed as affecting current authorities regarding the use or disclosure of information.

Subsection (b)

Subsection (a) adds a table of sections in Title 44—Information Security. Subsection (b) references other sections of related bills, including the Homeland Security Act of 2002, the National Institute of Standards and Technology Act, and the Cybersecurity Research and Development Act.

Subsection (c)

This subsection requires OMB to revise Appendix III of Office of Management and Budget Circular A–130 to eliminate inefficient or wasteful reporting. With this language, the Committee intends for OMB to rescind or amend Circular A–130 to eliminate the requirement for burdensome paperwork that does not provide cost-effective security.

This subsection ensures that the existing Information Security and Privacy Advisory Board, which currently advises NIST, also advises DHS.

Section 3. Federal data breach response guidelines

Section 201 adds a new section to Title 44: "Section 3559, Privacy breach requirements." This new section requires that the Director of OMB establish and oversee policies and procedures for agencies to follow in the event of a breach of personally identifiable information at an agency. It requires agencies to provide timely notice to

affected individuals, report to the federal information security incident center, provide notice to Congress, and perform other mitigation measures as required by the Director. Agencies are required to notify victims within 60 days, with law enforcement and national security exceptions. The Director must consider recommendations of the Government Accountability Office, including those found in GAO Report GAO–14–34, regarding OMB's policies for agency data breach notification practices and report to Congress annually to improve the consistency and effectiveness of government wide data breach response programs.

V. EVALUATION OF REGULATORY IMPACT

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 and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

VI. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

JULY 28, 2014.

Hon. TOM CARPER,
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. 2521, the Federal Information Security Modernization Act of 2014.

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. 2521—Federal Information Security Modernization Act of 2014

S. 2521 would amend the Federal Information Security Management Act of 2002 (FISMA)—the law that governs the security of the federal government's information technology systems. The legislation would clarify the roles and responsibilities of the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) for information security. The bill also would update guidelines that federal agencies follow in the event that there is an unauthorized release of data. S. 2521 would require OMB to revise Circular A–130—Management of Federal Information Resources.

CBO estimates that implementing S. 2521 would have no significant net impact on the federal budget over the next five years. The bill could affect direct spending by agencies not funded through annual appropriations; therefore, pay-as-you-go procedures apply. CBO estimates, however, that any net increase in spending by those agencies would not be significant. Enacting S. 2521 would not affect revenues.

Most of the provisions of the bill would codify and expand on current practices of the federal government. OMB has reported that in 2013, federal agencies spent almost $80 billion on information technology and more than $10 billion on related security.

S. 2521 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would impose no costs on state, local, or tribal governments budget.

The CBO staff contacts for this estimate are Matthew Pickford and Jason Wheelock. The estimate was approved by Theresa Gullo, Deputy Assistant Director for Budget Analysis.

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, changes in existing law made by S. 2521 as reported are shown as follows (existing law proposed to be omitted is enclosed in brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

TITLE 44, UNITED STATES CODE

* * * * * * *

CHAPTER 35 COORDINATION OF FEDERAL INFORMATION POLICY

* * * * * * *

[SUBCHAPTER II—INFORMATION SECURITY

[3531. Purposes.
[3532. Definitions.
[3533. Authority and functions of the Director.
[3534. Federal agency responsibilities.
[3535. Annual independent evaluation.
[3536. National security systems.
[3537. Authorization of appropriations.
[3538. Effect on existing law.]

[SUBCHAPTER III—INFORMATION SECURITY

[3541. Purposes.
[3542. Definitions.
[3543. Authority and functions of the Director.
[3544. Federal agency responsibilities.
[3545. Annual independent evaluation.
[3546. Federal information security incident center.
[3547. National security systems.
[3548. Authorization of appropriations.
[3549. Effect on existing law.

Subchapter II—Information Security]

Sec.
3551. Purposes.
3552. Definitions.
3553. Authority and functions of the Director and the Secretary.
3554. Federal agency responsibilities.
3555. Annual independent evaluation.
3556. Federal information security incident center.
3557. National security systems.
3558. Effect on existing law.
3559. Privacy breach requirements.

* * * * * * *

[Subchapter II—Information Security

[SEC. 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.'.

[SEC. 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.

[SEC. 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.

[SEC. 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 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 sys-

tems 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 agency-wide 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 agency-wide information security program, approved by the Director under section 3533(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 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 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, (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 poli-

cies and procedures to the extent that such policies and procedures affect communication with the public.

[SEC. 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, 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.

[SEC. 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.

[SEC. 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.

[SEC. 3538. 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 Congress or the Comptroller General of the United States.

[Subchapter III—Information Security

[SEC. 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 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; and

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

[SEC. 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 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 an appropriate level of information secrecy; and

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

[(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—

[(A) 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) 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); or

[(B) 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 secret in the interest of national defense or foreign policy; and

[(3) the term 'information technology' has the meaning given that term in section 5002 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401).

[SEC. 3543. AUTHORITY AND FUNCTIONS OF THE DIRECTOR.

[(a) 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 the promulgation of standards and guidelines under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441);

[(2) requiring agencies, consistent with the standards and guidelines promulgated under such section 5131 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 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 5113(b)(5) of the Clinger-Cohen Act of 1996 (40 U.S.C. 1413(b)(5)) to enforce accountability for compliance with such requirements;

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

[(6) overseeing the development and operation of the Federal information security incident center established under section 3536; and

[(7) reporting to Congress 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; and

[(C) planned remedial action to address such deficiencies.

[(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.

[SEC. 3544. 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 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 and guidelines promulgated by the Director under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441); 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 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 and guidelines promulgated under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441) 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 agency-wide 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 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441);

[(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 subparagraph (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 agency-wide information security program 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 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 subparagraph (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, including information security standards and guidelines promulgated under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441); and

[(iii) 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;

[(6) a process for ensuring 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 guidance issued under section 3536, including—

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

[(B) notifying and consulting with the Federal information security incident center established under section 3536; 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) Each agency shall—

[(1) report annually to the Director and the Comptroller General on the adequacy and effectiveness of information security policies, procedures, and practices, including compliance with the requirements of this subchapter;

[(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 the Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.);

[(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, (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, United States Code; 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.

[SEC. 3545. 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, 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 vulner-

ability 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) The results of an evaluation required by this section shall be submitted to the Director no later than March 1, 2003, and every March 1 thereafter.

[(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 a report to Congress.

[(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.

[SEC. 3546. FEDERAL INFORMATION SECURITY INCIDENT CENTER.

[(a) The Director shall cause to be established and operated 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 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) 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.

[SEC. 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 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.

[SEC. 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.]

SUBCHAPTER II—INFORMATION SECURITY

SEC. 3551. 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.

SEC. 3552. 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 "binding operational directive" means a compulsory direction to an agency that is in accordance with policies, principles, standards, and guidelines issued by the Director.

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

(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

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

(3) 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.

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

(5) The term "intelligence community" has the meaning given that term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(6)(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).

(7) The term "Secretary" means the Secretary of Homeland Security.

SEC. 3553. AUTHORITY AND FUNCTIONS OF THE DIRECTOR AND THE SECRETARY.

(a) DIRECTOR.—The Director shall oversee agency information security policies, 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) ensuring that the Secretary carries out the authorities and functions under subsection (b);

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

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

(7) consulting with the Secretary in carrying out the authorities and functions under this subsection.

(b) SECRETARY.—The Secretary, in consultation with the Director, shall oversee the operational aspects of agency information security policies and practices for information systems, except for national security systems and information systems described in paragraph (2) or (3) of subsection (e), including—

(1) assisting the Director in carrying out the authorities and functions under subsection (a);

(2) developing and overseeing the implementation of binding operational directives to agencies to implement the policies, principles, standards, and guidelines developed by the Director under subsection (a)(1) and the requirements of this subchapter, which may be repealed by the Director if the operational directives issued on behalf of the Director are not in accordance with policies, principles, standards, and guidelines developed by the Director, including—

(A) requirements for reporting security incidents to the Federal information security incident center established under section 3556;

(B) requirements for the contents of the annual reports required to be submitted under section 3554(c)(1);

(C) requirements for the mitigation of exigent risks to information systems; and

(D) other operational requirements as the Director or Secretary may determine necessary;

(3) monitoring agency implementation of information security policies and practices;

(4) convening meetings with senior agency officials to help ensure effective implementation of information security policies and practices;

(5) coordinating Government-wide efforts on information security policies and practices, including consultation with the Chief Information Officers Council established under section 3603;

(6) providing operational and technical assistance to agencies in implementing policies, principles, standards, and guidelines on information security, including implementation of standards promulgated under section 11331 of title 40, including by—

(A) operating the Federal information security incident center established under section 3556;

(B) upon request by an agency, deploying technology to assist the agency to continuously diagnose and mitigate against cyber threats and vulnerabilities, with or without reimbursement;

(C) compiling and analyzing data on agency information security; and

(D) developing and conducting targeted operational evaluations, including threat and vulnerability assessments, on the information systems; and

(7) other actions as the Secretary may determine necessary to carry out this subsection on behalf of the Director.

(c) REPORT.—Not later than March 1 of each year, the Director, in consultation with the Secretary, shall submit to Congress a report on the effectiveness of information security policies and practices during the preceding year, including—

(1) a summary of the incidents described in the annual reports required to be submitted under section 3554(c)(1), including a summary of the information required under section 3554(c)(1)(A)(iii);

(2) a description of the threshold for reporting major information security incidents;

(3) a summary of the results of evaluations required to be performed under section 3555;

(4) an assessment of agency compliance with standards promulgated under section 11331 of title 40; and

(5) an assessment of agency compliance with the policies and procedures established under section 3559(a).

(d) NATIONAL SECURITY SYSTEMS.—Except for the authorities and functions described in subsection (a)(4) and subsection (c), the authorities and functions of the Director and the Secretary under this section shall not apply to national security systems.

(e) DEPARTMENT OF DEFENSE AND INTELLIGENCE COMMUNITY 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 National 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 an element of the intelligence community, a contractor of an element of the intelligence community, or another entity on behalf of an element of the intelligence community that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of an element of the intelligence community.

SEC. 3554. 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;

(ii) operational directives developed by the Secretary under section 3553(b);

(iii) policies and procedures issued by the Director under section 3559; and

(iv) 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 agency-wide 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 3553 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;

(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;

(6) ensure that senior agency officials, including chief information officers of component agencies or equivalent officials, carry out responsibilities under this subchapter as directed by the official delegated authority under paragraph (3); and

(7) ensure that all personnel are held accountable for complying with the agency-wide information security program implemented under subsection (b).

(b) AGENCY PROGRAM.—Each agency shall develop, document, and implement an agency-wide information security program 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 3555;

(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 described in section 3556(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 established in section 3556; 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;

(iii) the committees of Congress described in subsection (c)(1)—

(I) not later than 7 days after the date on which the incident is discovered; and

(II) after the initial notification under subclause (I), within a reasonable period of time after additional information relating to the incident is discovered; and

(iv) 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.—

(1) ANNUAL REPORT.—

(A) IN GENERAL.—Each agency shall submit to the Director, the Secretary, the Committee on Government Reform, the Committee on Homeland Security, and the Committee on Science of the House of Representatives, the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General a report on the adequacy and effectiveness of information security policies, procedures, and practices, including—

(i) a description of each major information security incident or related sets of incidents, including summaries of—

(I) the threats and threat actors, vulnerabilities, and impacts relating to the incident;

(II) the risk assessments conducted under section 3554(a)(2)(A) of the affected information systems before the date on which the incident occurred; and

(III) the detection, response, and remediation actions;

(ii) the total number of information security incidents, including a description of incidents resulting in significant compromise of information security, system impact levels, types of incident, and locations of affected systems;

(iii) a description of each major information security incident that involved a breach of personally identifiable information, including—

(I) the number of individuals whose information was affected by the major information security incident; and

(II) a description of the information that was breached or exposed; and

(iv) any other information as the Secretary may require.

(B) UNCLASSIFIED REPORT.—

(i) IN GENERAL.—Each report submitted under subparagraph (A) shall be in unclassified form, but may include a classified annex.

(ii) ACCESS TO INFORMATION.—The head of an agency shall ensure that, to the greatest extent practicable, information is included in the unclassified version of the reports submitted by the agency under subparagraph (A).

(2) OTHER PLANS AND REPORTS.—Each agency shall address the adequacy and effectiveness of information security policies, procedures, and practices in management plans and reports.

(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)(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.

SEC. 3555. 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 of the effectiveness of the information security policies, procedures, and practices of the agency; 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, 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 3553(c).

(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) 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.

(i) ASSESSMENT TECHNICAL ASSISTANCE.—The Comptroller General may provide technical assistance to an Inspector General or the head of an agency, as applicable, to assist the Inspector General or head of an agency in carrying out the duties under this section, including by testing information security controls and procedures.

SEC. 3556. FEDERAL INFORMATION SECURITY INCIDENT CENTER.

(a) IN GENERAL.—The Secretary 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;

(4) provide, as appropriate, intelligence and other information about cyber threats, vulnerabilities, and incidents to agencies to assist in risk assessments conducted under section 3554(b); and

(5) 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.

SEC. 3557. NATIONAL SECURITY SYSTEMS.

The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system;

(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.

SEC. 3558. 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.

SEC. 3559. PRIVACY BREACH REQUIREMENTS.

(a) POLICIES AND PROCEDURES.—The Director, in consultation with the Secretary, shall establish and oversee policies and procedures for agencies to follow in the event of a breach of information security involving the disclosure of personally identifiable information, including requirements for—

(1) timely notice to affected individuals based on a determination of the level of risk and consistent with law enforcement and national security considerations;

(2) timely reporting to the Federal information security incident center established under section 3556 or other Federal cybersecurity center, as designated by the Director;

(3) timely notice to committees of Congress with jurisdiction over cybersecurity; and

(4) such additional actions as the Director may determine necessary and appropriate, including the provision of risk mitigation measures to affected individuals.

(b) CONSIDERATIONS.—In carrying out subsection (a), the Director shall consider recommendations made by the Government Accountability Office, including recommendations in the December 2013 Government Accountability Office report entitled "Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent" (GAO–14–34).

(c) REQUIRED AGENCY ACTION.—The head of each agency shall ensure that actions taken in response to a breach of information security involving the disclosure of personally identifiable information under the authority or control of the agency comply with policies and procedures established under subsection (a).

(d) TIMELINESS.—

(1) IN GENERAL.—Except as provided in paragraph (2), the policies and procedures established under subsection (a) shall require that the notice to affected individuals required under subsection (a)(1) be made without unreasonable delay and with consideration of the likely risk of harm and the level of impact, but not later than 60 days after the date on which the head of an agency discovers the breach of information security involving the disclosure of personally identifiable information.

(2) DELAY.—The Attorney General, the head of an element of the intelligence community (as such term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)), or the Secretary may delay the notice to affected individuals under subsection (a)(1) for not more than 180 days, if the notice would disrupt a law enforcement investigation, endanger national security, or hamper security remediation actions from the breach of information security involving the disclosure of personally identifiable information.

HOMELAND SECURITY ACT OF 2002

* * * * * * *

TITLE X—INFORMATION SECURITY

SEC. 1001. INFORMATION SECURITY.

(a) * * *

* * * * * * *

(c) INFORMATION SECURITY RESPONSIBILITIES OF CERTAIN AGENCIES.—

(1) NATIONAL SECURITY RESPONSIBILITIES—(A) Nothing in this Act (including any amendment made by this Act) shall su-

persede any authority of the Secretary of Defense, the Director of Central Intelligence, or other agency head, as authorized by law and as directed by the President, with regard to the operation, control, or management of national security systems, as defined by [section 3532(3)] *section 3552(b)* of title 44, United States Code.

* * * * * * *

TITLE 10, UNITED STATES CODE

* * * * * * *

Subtitle A—General Military Law

* * * * * * *

PART IV—SERVICE, SUPPLY, AND PROCUREMENT

* * * * * * *

CHAPTER 131—PLANNING AND COORDINATION

SEC. 2222. DEFENSE BUSINESS SYSTEMS: ARCHITECTURE, ACCOUNTABILITY, AND MODERNIZATION.

(a) * * *

* * * * * * *

(j) DEFINITIONS.—In this section:

(1) * * *

* * * * * * *

(5) The term "national security system" has the meaning given that term in [section 3542(b)(2)] *section 3552(b)* of title 44.

* * * * * * *

SEC. 2223. INFORMATION TECHNOLOGY: ADDITIONAL RESPONSIBILITIES OF CHIEF INFORMATION OFFICERS.

(a) * * *

* * * * * * *

(c) DEFINITIONS.—

(1) * * *

* * * * * * *

(3) The term "national security system" has the meaning given that term by [section 3542(b)(2)] *section 3552(b)* of title 44.

* * * * * * *

CHAPTER 137—PROCUREMENT GENERALLY

* * * * * * *

SEC. 2315. LAW INAPPLICABLE TO THE PROCUREMENT OF AUTOMATIC DATA PROCESSING EQUIPMENT AND SERVICES FOR CERTAIN DEFENSE PURPOSES.

For purposes of subtitle III of title 40, the term "national security system", with respect to a telecommunications and information system operated by the Department of Defense, has the meaning given that term by [section 3542(b)(2)] *section 3552(b)* of title 44.

* * * * * * *

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ACT

* * * * * * *

SEC. 20. (a) The Institute shall—

(1) * * *

(2) develop standards and guidelines, including minimum requirements, for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, other than national security systems (as defined in [section 3532(b)(2)] *section 3552(b)* of title 44, United States Code);

* * * * * * *

(e) As used in this section—

(1) * * *

(2) the term "information security" has the same meaning as provided in [section 3532(1)] *section 3552(b)* of such title;

* * * * * * *

(5) the term "national security system" has the same meaning as provided in [section 3532(b)(2)] *section 3552(b)* of such title.

* * * * * * *

CYBER SECURITY RESEARCH AND DEVELOPMENT ACT

* * * * * * *

SEC. 8. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY PROGRAMS.

(a) * * *

* * * * * * *

(d) FEDERAL AGENCY INFORMATION SECURITY PROGRAMS.—

(1) IN GENERAL.—In developing the agency-wide information security program required by [section 3534(b)] *section 3554(b)* of title 44, United States Code, an agency that deploys a computer hardware or software system for which the Director of the National Institute of Standards and Technology has developed a checklist under subsection (c) of this section—

(A) * * *

* * * * * * *

○