Calendar No. 674

118TH CONGRESS *2d Session*	SENATE	REPORT 118–271

FEDERAL INFORMATION SECURITY MODERNIZATION ACT (FISMA) OF 2023

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 2251

TO IMPROVE THE CYBERSECURITY OF THE FEDERAL GOVERNMENT, AND PUBLIC HEALTH SECTOR

DECEMBER 9, 2024.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
59–010 WASHINGTON : 2025

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware	RAND PAUL, Kentucky
MAGGIE HASSAN, New Hampshire	RON JOHNSON, Wisconsin
KYRSTEN SINEMA, Arizona	JAMES LANKFORD, Oklahoma
JACKY ROSEN, Nevada	MITT ROMNEY, Utah
JON OSSOFF, Georgia	RICK SCOTT, Florida
RICHARD BLUMENTHAL, Connecticut	JOSH HAWLEY, Missouri
LAPHONZA R. BUTLER, California	ROGER MARSHALL, Kansas

DAVID M. WEINBERG, *Staff Director*
ALAN S. KAHN, *Chief Counsel*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
EMILY A. FERGUSON, *Professional Staff Member*
WILLIAM E. HENDERSON III, *Minority Staff Director*
CHRISTINA N. SALAZAR, *Minority Chief Counsel*
ANDREW J. HOPKINS, *Minority Counsel*
KENDAL B. TIGNER, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 674

118TH CONGRESS *2d Session* | SENATE | REPORT 118–271

FEDERAL INFORMATION SECURITY MODERNIZATION ACT (FISMA) OF 2023

DECEMBER 9, 2024.—Ordered to be printed

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

R E P O R T

[To accompany S. 2251]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 2251) to improve the cybersecurity of the Federal Government, and for other purposes, having considered the same, reports favorably thereon with an amendment, in the nature of a substitute, and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

S. 2251, the *Cybersecurity Act of 2023* includes two bills, the *Federal Information Security Modernization Act of 2023* (FISMA 2023) and the *Hospital Cybersecurity Enhancement Act*. FISMA 2023 revises and updates the Federal Information Security Modernization Act of 2014 (FISMA 2014) to support a more effective federal cybersecurity regime and improve cybersecurity coordination between the Office of Management and Budget (OMB), the Cybersecurity and Infrastructure Agency (CISA), the Office of the National Cyber

Director (NCD), and other federal agencies and contractors. The bill reforms how federal agencies report and respond to cyber-attacks, codifies and expands security priorities such as zero trust architecture, and enhances logging and detection capabilities. FISMA 2023 also significantly updates congressional oversight mechanisms for cybersecurity incidents that occur at federal agencies. The *Rural Hospital Cybersecurity Enhancement Act* was separately introduced as S. 1560 and separately considered by the Senate Committee on Homeland Security and Governmental Affairs on June 14, 2023. The *Rural Hospital Cybersecurity Enhancement Act* in title II of the *Cybersecurity Act of 2023* is the same as the language separately considered by the Committee.[1]

II. Background and Need for the Legislation

The United States' federal cybersecurity posture has left America's data at risk.[2] Despite reforms to federal cybersecurity codified in FISMA 2014, federal agencies continue to receive poor marks for cybersecurity.[3] Attacks in recent years, such as the Chinese actor Storm-0558 attack that gained access to email accounts of several cabinet secretaries and the Russian government attack on SolarWinds have led to compromises of federal government agencies and have shown the vulnerability of federal information systems to hackers, underscoring the urgent need for federal cybersecurity reforms.[4]

The Senate Homeland Security and Governmental Affairs Committee thoroughly examined the issues surrounding federal cybersecurity, hosted multiple hearings and published a report during the 117th Congress.[5] These hearings and report illuminated several themes that FISMA 2023 works to address, including:

- The need for improved congressional oversight over agency cybersecurity incidents;
- The benefits of integrating federal cybersecurity by breaking down silos between agencies;

---

[1] Additional information on the Rural Hospital Cybersecurity Enhancement Act can be found in the committee report for S. 1560. (Senate Homeland Security and Governmental Affairs Committee, Report to Accompany S. 1560, Rural Cybersecurity Enhancement Act (May 2023) (S. Report 118–170).

[2] Senate Committee on Homeland Security and Governmental Affairs, *Federal Cybersecurity: America's Data Still At Risk* (Aug. 2021).

[3] Senate Committee on Homeland Security and Governmental Affairs, *Federal Cybersecurity: America's Data Still At Risk* (Aug. 2021); Government Accountability Office, *Preliminary Results Show That Agencies' Implementation of FISMA Requirements Was Inconsistent* (GAO–22–105637) (Jan. 11, 2022); Government Accountability Office, *OMB Should Improve Information Security Performance Metrics* (GAO–24–106291) (Jan. 9, 2024).

[4] Charlie Bell, *Mitigation for China-based threat actor activity*, Microsoft (blog) (Jul 11, 2023) (blogs.microsoft.com/on-the-issues/2023/07/11/mitigation-china-based-threat-actor/).; *Chinese Hackers Targeted Commerce Secretary and Other U.S. Officials*, NYTimes (Jul. 12, 2023) (www.nytimes.com/2023/07/12/us/politics/china-state-department-emails-microsoft-hack.html).; *SolarWinds recap: All of the federal agencies caught up in the Orion breach*, FEDSCOOP (Dec. 22, 2020) (www.fedscoop.com/solarwinds-recap-federal-agencies-caught-orion-breach/).

[5] Senate Committee on Homeland Security and Governmental Affairs, *Hearing on GAO's 2021 High Risk List: Addressing Waste, Fraud, and Abuse*, 117th Cong. (Mar. 2, 2021) (S. Hrg. 117–424).; Senate Committee on Homeland Security and Governmental Affairs, *Hearing on Understanding and Responding to the SolarWinds Supply Chain Attack: The Federal Perspective* (Mar. 18, 2021) (S. Hrg. 117–478).; Senate Committee on Homeland Security and Governmental Affairs, *Hearing on Prevention, Response, and Recovery: Improving Federal Cybersecurity Post-SolarWinds* (May 11, 2021) (S. Hrg. 117–478).; Senate Committee on Homeland Security and Governmental Affairs, *Hearing on National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems* (Sep. 23, 2021) (S. Hrg. 117–266).; Senate Committee on Homeland Security and Governmental Affairs, *Federal Cybersecurity: America's Data Still At Risk* (Aug. 2021).

- The importance of the NCD and CISA, and the need to codify their federal cybersecurity roles; and
- The benefits of taking a risk-based approach to cybersecurity, and to allocate resources away from burdensome reporting requirements.

FISMA 2023 addresses these issues by building upon and updating FISMA 2014, specifically to recognize and clearly define the roles of two federal entities that did not exist when FISMA 2014 was signed into law: CISA as the lead agency for operational federal cybersecurity support and the NCD serving as the lead cybersecurity advisor to the President for strategy and budgeting priorities.[6] These two new offices, along with OMB, are tasked with breaking down the silos between agencies by being required to consult on various agency cybersecurity plans and investments.[7] They are also tasked with centralizing analysis of incident data, to reduce the burden on each agency and enable federal-wide analysis of cyber-attacks.[8]

Under FISMA 2014, Congress is required to be notified when an agency experiences a "major incident"—a subset of all cybersecurity incidents that reach an OMB defined threshold of significance.[9] Congress received zero major incident reports in Fiscal Year (FY) 2018, out of a total of 31,107 cybersecurity incidents at agencies. In FY 2019, 3 major incidents were reported, and in FY 2020 6 major incidents were reported, with about 30,000 total agency incidents occurring in each of those two years.[10] The trend of increasing major incidents has continued; FY 2023 saw 11 major incidents reported out of 32,000 total agency incidents.[11] One of the recommendations from the Committee's report on FISMA was the need to define "major incidents" such that Congress is notified in a consistent and timely manner, rather than continue to rely on OMB's current definition which has led to inconsistent notifications.[12] FISMA 2023 addresses this issue by explicitly defining the thresholds for "major incidents" that need to be reported to Congress.

The major incident definition in FISMA 2023 builds on the existing definition established by the OMB. The existing definition focuses on national security and national health, safety and privacy of the public. The FISMA 2023 language includes cyber incidents that impact an agency's ability to deliver a critical service, that im-

---

[6] 44 U.S.C. § 3552; Pub. L. 113–283; Executive Office of the President, *National Security Memorandum on Critical Infrastructure Security and Resilience* (NSM–22) (April 30, 2024).

[7] Pub. L. 115–278; Executive Office of the President, *National Cybersecurity Strategy* (March 2023) (www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf).

[8] *Id.*

[9] Under FISMA 2014, the definition of a cybersecurity incident is "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. FISMA 2014 also gives OMB the authority to set the definition of a "major incident" without any additional specifications on what the threshold should include. 44 U.S.C. § 3552; Pub. L. 113–283, § 2(b).

[10] Executive Office of the President, *Federal Information Security Modernization Act of 2014 Annual Report to Congress Fiscal Year 2018* (Sep. 2019).; Executive Office of the President, *Federal Information Security Modernization Act of 2014 Annual Report to Congress Fiscal Year 2019* (May 2020).; *Executive Office of the President, Federal Information Security Modernization Act of 2014 Annual Report to Congress Fiscal Year 2020* (May 2021).

[11] Executive Office of the President, *Federal Information Security Modernization Act of 2014 Annual Report to Congress Fiscal Year 2023* (May 2024).

[12] Senate Committee on Homeland Security and Governmental Affairs, *Federal Cybersecurity: America's Data Still At Risk* (Aug. 2021).

pact high value assets agencies, and require notification when sensitive agency information is exposed to a foreign entity.

The existing major incident definition, and the definition at the time of the SolarWinds incident, as established by OMB pursuant to FISMA 2014, do not include any requirements for reporting incidents impacting multiple agencies.[13] The updated major incident definition also requires the NCD to declare a major incident at each impacted agency if a common root cause leads to incidents at multiple agencies, as occurred during the SolarWinds incident.[14] During the SolarWinds compromise, some agencies declared major incidents to Congress, while others who were publicly reported to have been impacted, did not. Inconsistencies in applying the major incident standard also led agencies to at times delay notification to Congress. These issues led to then-Ranking Member Peters sending letters to 26 agencies requesting information about their status with respect to the vulnerability and if they had experienced any resulting cybersecurity incidents, for lack of any other mechanism to determine the full impact to the Federal ecosystem.[15]

The updated major incident definition in FISMA 2023 differs from OMB's existing definition by not including reporting requirements to Congress when personally identifiable information is breached. Instead, the bill includes a separate section dedicated to personally identifiable information breaches, with updated reporting thresholds and requirements for notifying Congress and potentially impacted individuals when personal information breaches occur. This separation of congressional notification requirements will allow agencies to independently assess congressional reporting thresholds for personally identifiable information breaches and cyber-attacks. It also clarifies that breaches that occur *not* due to a cyber-attack are still required to be reported to Congress when certain thresholds are met.

FISMA 2023 also moves agencies towards a risk-based approach, while reducing resources dedicated to reporting metrics. Each agency is required to perform an ongoing and continuous agency risk assessment, and CISA is required to consolidate this work to perform federal-wide risk assessments. These assessments will be required to be incorporated into agency resource allocations for cybersecurity investments. The bill shifts existing agency annual FISMA reports to be transmitted every two years, and requires agencies move to automation for information sharing throughout the legislation.

---

[13] Office of Management and Budget, *Fiscal Year 2019–2020 Guidance on Federal Information Security and Privacy Management Requirements* (M–20–04) (Nov. 2019).; Office of Management and Budget, *Fiscal Year 2020–2021 Guidance on Federal Information Security and Privacy Management Requirements* (M–21–02) (Nov. 2020).

[14] *SolarWinds recap: All of the federal agencies caught up in the Orion breach*, FEDSCOOP (Dec. 22, 2020) (www.fedscoop.com/solarwinds-recap-federal-agencies-caught-orion-breach/).

[15] Letters from Ranking Member Gary C. Peters to the heads of the following agencies: Department of Health and Human Services, Environmental Protection Agency, Department of Housing and Urban Development, Department of Homeland Security, Federal Emergency Management Agency, Department of Defense, Department of Energy, Department of the Interior, Department of Transportation, General Services Administration, Department of Labor, Department of Justice, National Aeronautics and Space Administration, United States Agency for International Development, Small Business Administration, U.S. Nuclear Regulatory Commission, Department of State, Office of Personnel Management, Department of Education, Department of Veterans Affairs, Office of Management and Budget, Office of the Director of National Intelligence, National Science Foundation, Department of Agriculture, Department of Treasury, and Department of Commerce (Feb. 21, 2019).

Finally, several provisions of FISMA 2023 are based on Executive Order No. 14028 and other executive branch mandates to require agencies to move towards modern cybersecurity practices, including increased use of automation, moving network security to Zero Trust Architectures using principles of least privilege, increased use of penetration testing, and establishing vulnerability disclosure programs at all agencies.[16]

III. LEGISLATIVE HISTORY

Chairman Gary Peters (D–MI) and Senator Josh Hawley (R–MO) introduced S. 2251, the *Federal Information Security Modernization Act of 2023*, on July 11, 2023. The bill was referred to the Committee on Homeland Security and Governmental Affairs. The Committee considered S. 2251 at a business meeting held on Wednesday, July 26, 2023.

During the business meeting, Chairman Peters offered a substitute amendment to the bill as well as a modification to the substitute amendment. The Peters substitute amendment, as modified, changed the short title of the bill to the *Cybersecurity Act of 2023*, moved FISMA 2023 into Title I, added the *Rural Hospital Cybersecurity Enhancement Act* as Title II, added an additional provision in FISMA 2023's rule of construction to clarify that nothing in the title may be construed to impinge on the privacy rights of individuals or allow the unauthorized access, sharing, or use of personal data, and additional technical corrections to FISMA 2023. The Committee adopted the modification to the Peters substitute by unanimous consent, with Senators Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Blumenthal, Paul, Lankford, Romney, Scott, Hawley, and Marshall present. The Peters substitute amendment, as modified, was adopted by unanimous consent, with Senators Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Blumenthal, Paul, Lankford, Romney, Scott, Hawley, and Marshall present.

Ranking Member Paul offered Paul Amendment 13, which would add the text of S. 2425, the *Free Speech Protection Act* at the end of S. 2251. Ranking Member Paul offered a modification to the amendment that that would strike all sections except for the definitions, employee prohibitions, reporting requirements, and applicability of FOIA. The modification also struck the requirement for DHS to terminate the Disinformation Governance Board and removed the prohibition on Executive agencies awarding grants related to programming on misinformation or disinformation. The modification to Paul Amendment 13 was adopted by unanimous consent with Senators Peters, Hassan, Sinema, Rosen, Ossoff, Paul, Lankford, Romney, Scott, and Hawley present. Paul Amendment 13, as modified, was not adopted by roll call vote of 6 yeas to 9 nays, with Senators Paul, Lankford, Scott, and Hawley voting in the affirmative and Senators Peters, Hassan, Sinema, Rosen, Ossoff, and Romney voting in the negative. Senators Johnson and Marshall voted yea by proxy, and Senators Carper, Padilla, and Blumenthal voted nay by proxy.

---

[16] Cybersecurity and Infrastructure Security Agency, *Binding Operational Directive 20–01—Develop and Publish a Vulnerability Disclosure Policy* (BOD–20–01) (Sep. 2020).; Exec. Order No. 14028, 86 Fed. Reg. 26633 (May 12, 2021).

Ranking Member Paul offered Paul Amendment 15, which would prohibit CISA from directly or indirectly monitoring communications or partake in electronic surveillance, including monitoring of federal agency systems where CISA has responsibility and agreements with other agencies to monitor for cybersecurity incidents or cybersecurity vulnerabilities, unless expressly authorized by law or a court. Paul Amendment 15 was not adopted by roll call vote of 7 yeas to 8 nays, with Senators Paul, Lankford, and Hawley voting in the affirmative and Senators Peters, Hassan, Sinema, Rosen, Padilla, and Ossoff voting in the negative. Senators Johnson, Marshall, Romney, and Scott voted yea by proxy, and Senators Carper and Blumenthal voted nay by proxy.

Ranking Member Paul offered Paul Amendment 28, which would require privacy impact assessments (PIAs) be conducted prior to the implementation of any new cybersecurity measure, expanding the requirement for PIAs beyond current processes and policy. Paul Amendment 28 was not adopted by roll call vote of 5 yeas to 10 nays, with Senators Paul and Hawley voting in the affirmative and Senators Peters, Hassan Sinema, Rosen, Padilla, and Lankford voting in the negative. Senators Johnson, Scott, and Marshall voted yea by proxy, and Senators Carper, Ossoff, Blumenthal, and Romney voted nay by proxy.

Ranking Member Paul offered Paul Amendment 51, which would strike the provision allowing an incumbent in the Federal Chief Information Security Officer role to maintain their position without a new presidential appointment, and replace at provision with a requirement require the Federal Chief Information Security Officer be Senate-confirmed and no person may act in the capacity of the position without confirmation. Paul Amendment 51 was not adopted by roll call vote of 6 yeas to 9 nays, with Senators Paul, Lankford, and Hawley voting in the affirmative and Senators Peters, Hassan Sinema, Rosen, and Padilla voting in the negative. Senators Johnson, Scott, and Marshall voted yea by proxy, and Senators Carper, Ossoff, Blumenthal, and Romney voted nay by proxy.

Ranking Member Paul offered Paul Amendment 64, which would (1) allow any agency Chief Information Security Officer to remove a CISA liaison to the agency without cause or reason, (2) require PIAs be conducted prior to the implementation of any new cybersecurity measure, (3) require annual audits of CISA liaisons and their alignment with federal and state privacy laws, (4) prohibiting CISA liaisons from engaging in domestic collection or surveillance activities including collection of relevant cybersecurity incident information from agency networks, (5) prohibiting CISA liaisons from logging, tracking, monitoring, categorizing, analyzing, retaining, or in any way use data or content on the basis of political viewpoint, (6) require liaisons to prioritize the protection of personal data of U.S. citizens, (7) prohibiting CISA liaisons from using any resources provided to the liaison to carry out any domestic collection or surveillance activity, including potential collection of cybersecurity threat information on federal information systems, and requiring the termination of any liaison who misuses such resources, and (8) requiring the Inspector General of DHS to conduct semi-annual reviews of the activities of each liaison and to report such reviews to relevant congressional committees.

Ranking Member Paul offered to modify Amendment 64. The modification to Paul 64, which would remove the ability of an agency CISO to request the removal of CISA liaisons to the agency, was adopted by unanimous consent with Senators Peters, Hassan, Sinema, Rosen, Padilla, Paul, Lankford, and Hawley present. Paul Amendment 64 as modified was not adopted by roll call vote of 6 yeas to 9 nays, with Senators Paul, Lankford, and Hawley voting in the affirmative and Senators Peters, Hassan, Sinema, Rosen, and Padilla voting in the negative. Senators Johnson, Scott, and Marshall voted yea by proxy, and Senators Carper, Ossoff, Blumenthal, and Romney voted nay, by proxy.

The bill, as amended by the Peters substitute amendment, as modified, was ordered reported favorably by roll call vote of 8 yeas and 1 nay, with Senators Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Lankford, and Hawley voting in the affirmative and Senator Paul voting in the negative. Senators Carper, Blumenthal, and Romney voted yea by proxy, and for the record only, and Senators Johnson, Scott, and Marshall voted nay by proxy, and for the record only.

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

Section 1. Short title; Table of contents

This section designates the short title of the bill as the "Cybersecurity Act of 2023" and contains the table of contents.

TITLE I—FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2023

Section 101. Short title

This section designates title I as the "Federal Information Security Modernization Act of 2023."

Section 102. Definitions

This section defines "agency," "appropriate congressional committees," "Awardee," "Contractor," "Director," "Federal information system," "incident," "national security system," "penetration test," "threat hunting," and "zero trust architecture."

Section 103. Amendments to Title 44

This section amends sections within title 44, U.S. Code. Subsection (a) amends U.S. Code sections in subchapter I of chapter 35 of title 44. Subsection (a)(1) amends 44 U.S.C. § 3504. It requires the Director of the Office of Management and Budget (OMB) to consult with the National Cyber Director (NCD) when developing and overseeing the implementation of policies, principles, standards, and guidelines on information security. Subsection (a)(2) amends 44 U.S.C. § 3505. It strikes a duplicate subsection related to system inventorying and updates the remaining inventory to require the identification of internet accessible information systems. It also adds the NCD and the Director of CISA to the list of individuals who receive a copy of the inventory of agency IT systems conducted by OMB, and requires the inventory be maintained on a continual basis, through the use of automation wherever practicable. Subsection (a)(3) amends 44 U.S.C. § 3506. It requires agencies to improve the availability of information resources and

also requires agencies to promote security with respect to Federal information technology. (a)(3) also instructs the Chief Information Officer to consult with the Chief Data Officer to accomplish these goals. It also directs each agency to designate a Chief Privacy Officer, in accordance with section 552(a) of division H of the Consolidated Appropriations Act, 2005 (42 U.S.C. 2000ee–2), and authorizes specific responsibilities for the officer. Subsection (a)(4) amends 44 U.S.C. § 3513. It requires agencies to provide any portion of a written plan, developed in response to an OMB review under § 3513(a), addressing information security or cybersecurity to the National Cyber Director and Secretary of Homeland Security.

Subsection (b) amends definitions in U.S. Code subchapter II of chapter 35 of title 44. (b)(1) amends 44 U.S.C. § 3552(b). It adds several definitions, including "high value asset," "major incident," "penetration test," "shared service," and "zero trust architecture." (b)(2) contains a number of conforming amendments to align scattered Federal statutes with the updated definitions in § 3552.

Subsection (c) amends U.S. Code sections in subchapter II of chapter 35 of title 44. (c)(1) amends 44 U.S.C. § 3551. It recognizes that OMB, CISA, NCD, and other agencies have a specific mission when dealing with cybersecurity and resources vary across the federal government. It also recognizes that a holistic federal cybersecurity model is necessary to help account for these differences. (c)(2) amends 44 U.S.C. § 3553. This subsection requires agencies to submit FISMA reports every two years, instead of every year. It also amends existing law to require OMB to now consult with CISA and the NCD on a number of federal information security issues—detailed below. The section requires OMB consult with CISA and NCD to oversee agency information security policies and practices, including overseeing agency compliance. It also requires OMB to work with NCD, CISA and NIST to promote the use of automation and least privilege principles, such as zero trust architecture, to improve cybersecurity resilience and response time. It also specifies that OMB and NCD will collaborate with CISA to seek methods to reduce costs and administrative burdens through shared cybersecurity services. It also specifies that CISA, in consultation with the NCD and OMB, will administer the implementation of agency information security policies and practices, monitor implementation, lead coordination, perform penetration testing, and provide technical and operational assistance to agencies. (c)(2) also requires CISA to perform ongoing and continuous assessments of Federal cybersecurity risk posture, using a variety of information sources, and to brief OMB and NCD on those assessments. It also directs the Director of OMB to include a summary of the federal risk posture assessed by CISA in its FISMA report to Congress. This subsection also requires CISA to report to appropriate reporting entities, including Congress, on agency status of implementing Emergency Directives (first within 7 days with 30-day updates) and Binding Operational Directives (first within 30 days with 90-day updates) issued by the Secretary of DHS. OMB and GAO are also directed to review the efficacy of OMB issued information security guidance and policies once every 3 years. NIST is directed to develop, as appropriate, specifications to enable agencies to automate the verification of NIST-required controls, and CISA is required to provide federal risk assessment information to the Inspector Gen-

eral of the Department of Homeland Security and other appropriate IG's upon request. (c)(3) amends 44 U.S.C. § 3554. This subsection requires agency heads to on an ongoing and continuous basis, assess agency risk, specifies what must be included in that assessment, and requires that updates on that assessment to be provided to OMB, CISA, the NCD, and upon request, the Comptroller General. (c)(3) also aligns later sections of § 3554 with the updated risk assessment, implementation plan, and other programs added by the bill, including ensuring compliance with operational directives, creating acceptable system configuration requirements, and creating a process for providing the status of remedial actions and known system vulnerabilities to CISA. (c)(3) also changes existing law by requiring each agency to submit a biennial report, rather than an annual report summarizing its annual risk assessment, evaluating the effectiveness of cybersecurity policies, and summarizing the status of remedial actions identified by the agency Inspector General, GAO, or any other source to OMB, DHS, congressional leadership, relevant congressional committees, the NCD, and GAO. The subsection directs that, to the greatest extent practicable, those reports should be unclassified, but may include 1 or more annexes that contain classified or sensitive information. (c)(3) also mandates that OMB provide a briefing to congressional committees the years a report is not required. Finally, (c)(3) requires each agency to identify a Chief Information Security Officer to manage information security, cybersecurity budgets, and risk and compliance activities. (c)(4) amends 44 U.S.C. § 3555. This subsection changes the independent evaluations of agency information security programs and practices from yearly to biennial (in line with the change to have agencies submit biennial rather than annual FISMA reports to Congress). It also instructs OMB to identify any entity performing this independent audit in OMB's summary report to Congress of these evaluations. (c)(4) further requires that the guidance developed by the OMB Director to evaluate the effectiveness of an information security program and practices will prioritize the identification of the most common threat patterns experienced by each agency and the security controls that address those patterns, and any other security risks unique to the networks of each agency. This subsection also explicitly allows IGs to perform, or review results of, agency penetration testing. (c)(5) amends 44 U.S.C. § 3556(a) to require the existing reference to a federal information security incident center be maintained at CISA.

Subsection (d) makes conforming amendments to update the table of sections and update other references to FISMA reports to be submitted every two years, instead of every year, as changed in § 3553.

Subsection (e)(1) amends U.S. Code by adding a new subchapter IV, Federal System Incident Response, to chapter 35 of title 44. § 3591 defines "appropriate reporting entities," "awardee," "breach," "contractor," "Federal information," "Federal information system," "intelligence community," "nationwide consumer reporting agency," and "vulnerability disclosure." It also imports definitions from sections 3502 and 3552. 44 U.S.C. § 3592 requires agency heads to expeditiously determine whether notice to individuals potentially impacted by a cybersecurity breach is appropriate based on the nature and sensitivity of the breached information and, if appro-

priate, give written notice to those individuals within 45 days after the agency has concluded that such an incident occurred. The section specifies the contents of the notification and allows the head of an agency in coordination with OMB and the National Cyber Director, and as appropriate, with the Attorney General, Director of National Intelligence, or Secretary of Homeland Security to delay the notification if it would impede a criminal investigation, reveal sensitive sources and methods, cause damage to national security, or hamper security remediation actions. If there is a significant change in the details of the information that must be provided to impacted individuals, the agency must notify those individuals within 30 days. This section also requires Congress be notified whenever an agency makes a determination to notify potentially impacted individuals of a breach or if a breach impacts more than 50,000 individuals. This section also requires the head of an agency to submit annual reports to Congress regarding any delays of notifications or determinations to not provide notifications from the prior two years. 44 U.S.C. § 3593 requires agencies to provide written notification to the appropriate congressional entities within 72 hours after the agency has reasonable basis to conclude that a major incident occurred. It specifies the appropriate congressional leadership and committees the report must be submitted to and the content of the notification. It also requires a supplemental written update within 30 days after the initial written notification and requires the agency to provide an update report if there is any significant change in the agency's understanding of the incident after the supplemental update. The section also requires notifications and updates be submitted to Congress electronically, and unclassified (allowing for classified annexes) and clarifies that applicable breach reporting requirements under 3592 may be submitted to Congress under this section, or under processes established in 3592. Finally, the section requires the NCD to make recommendations to agencies on formatting and content of congressional notifications to improve consistency, and for the NCD to maintain a comprehensive record of all major incident notifications to be provided to Congress, upon request. § 3594 requires agency heads to provide any information on any incident to CISA (except incidents that are exclusively on national security systems) and specifies the contents of that communication. This section also requires the CISA Director make the information received available to OMB, NCD, and any other agency that may be impacted. It also requires each agency that has experienced a major incident, not including incidents on national security systems, to consult with CISA regarding response, recovery, and mitigation. It requires each agency that operates or exercises control of a national security system to report information of incidents with the National Manager for National Security Systems and CISA, as appropriate.

44 U.S.C. § 3595 imposes responsibilities on Federal contractors and awardees who have experienced cyber incidents or breaches involving Federal information or Federal systems to report to the contracting or grantor agency. This section requires the agency to share any incident information with CISA. This section requires contractors to report no later than 1 day after identification of an incident or a vulnerability that has been exploited. It requires reporting no later than 90 days after identification of a vulnerability

reported to the contractor by a third party. This section becomes effective one year after enactment and requires OMB to issue guidance for agencies on the scope of vulnerabilities to be reported. The Federal Acquisition Regulatory Council and Office of Federal Financial Management are directed to promulgate regulations relating to contractors to comply with the requirements set forth in this section. The head of each agency must implement these regulations and policies where appropriate and notify OMB of policies necessary to implement these regulations. OMB is also required to report to Congress the status of each agency's implementation of these regulations.

44 U.S.C. § 3596 directs agencies to develop training for individuals at the agency who obtain access to Federal information as an employee, contractor, awardee, volunteer, or intern to identify and respond to cyber incidents, and includes requirements for the contents of those trainings. This section also requires CISA, OMB, NCD, and NIST to provide best practices to agencies on developing these trainings. It also directs that this training may be included in an annual agency privacy or security awareness training. § 3597 requires CISA to perform continuous quantitative and qualitative analysis of incidents at federal agencies. It directs that this analysis should be automated to the greatest extent practicable. It directs OMB to share this information with agencies and the NCD to support and improve their cybersecurity efforts, specifies a format for that analysis. This section also directs CISA to produce an annual report on all federal incidents beginning not later than two years after enactment, for both Congress and public release. The section requires that information contained in the public report must be anonymized to prevent identification of specific incidents with specific agencies unless OMB, the impacted agency, and the relevant OIG are consulted. Finally, the section directs agencies that do not provide all incident data to CISA pursuant to 3594(a) to develop and provide to the appropriate notification entities, in coordination with CISA and OMB, their own annual report including data not provided to CISA that meets the requirements in this section.

44 U.S.C. § 3598 requires the Director of OMB, in coordination with the Director of the NCD, to issue guidance on the definition of "major incident" 1 year after the enactment of this bill or 1 year after publication of OMB's previous guidance to agencies regarding major incidents. It also provides requirements for elements that, at a minimum, should be included in the guidance and scenarios where a major incident determination should be made by the head of an agency or the NCD. These include areas such as national security, homeland security, impacts to civil liberties, public confidence, privacy, public health, and degradation of agency systems or operations.

Subsection (e)(2) amends U.S. Code by amending the table of sections for chapter 35 of title 44.

Section 104. Amendments to Subtitle III of Title 40

This section amends several sections within title 40 U.S. Code. Subsection (a) amends 40 U.S.C. § 11301 note. It requires the Technology Modernization Fund (TMF) consider using funds to improving cybersecurity and requires, as appropriate, TMF proposals in-

clude a cybersecurity risk management plan and supply chain risk management plan. This subsection also adds CISA to the TMF board.

Subsection (b) amends 40 U.S.C. § 11302. It requires that the Director of CISA and the NCD be consulted about promoting and improving the security of information technology used by the Federal Government. It also requires agencies consider if a function could be performed by a shared service from another agency, prior to making an acquisition.

Subsection (c) amends 40 U.S.C. § 11312, 11313, 11317, and 11319 by adding security considerations into the acquisition and resource management planning activities of agencies.

Section 105. Actions to enhance Federal incident transparency

Subsection (a) requires that CISA develop a plan for the analysis required under 44 U.S.C. 3597(a) that will include a description of any anticipated challenges, and the use of automation and machine readable formats for monitoring and analyzing data. It also requires CISA to brief appropriate congressional committees on the plan.

Subsection (b) requires the Director of OMB to develop guidelines and templates for agencies' implementation of the U.S. Code sections amended by this act, including § 44 U.S.C. 3594(a), § 3594(c), § 3595, and § 3596. It also requires OMB to coordinate with CISA in developing guidance on incident data sharing.

Subsection (c) amends 5 U.S.C. § 552a(b), the "Privacy Act of 1974" to clarify that when disclosure of information to another federal agency is warranted to facilitate a response to a cybersecurity incident, or to share incident information with CISA, a federal agency may provide it.

Section 106. Additional guidance to agencies on FISMA updates

This section requires the Director of OMB to issue guidance on: Performing the ongoing and continuous agency risk assessment required under law being amended by this Act; Establishing a process for providing a status of remedial actions for high value assets to OMB and CISA. Coordination with agency OIGs to ensure understanding and application of agency policies for the purpose of agency OIG evaluations; and

Section 107. Agency requirements to notify private sector entities impacted by incidents

This section directs the Director of OMB, in consultation with the National Cyber Director, to issue guidance, not later than 1 year after the enactment of this act. that requires agencies to notify private sector entities of cybersecurity incidents impacting the sensitive information shared by that entity.

Section 108. Mobile security briefings

Subsection (a) requires OMB to provide briefings to Congress on agency compliance with the No TikTok on Government Devices Act. Additionally, OMB must provide to Congress a list of all agency exceptions to the No TikTok on Government Devices Act, which may include a classified annex.

Subsection (b) requires OMB to provide briefings to all appropriate congressional committees detailing the compliance status of any agency found not to comply with the No TikTok on Government Devices Act at the time of the briefing in subsection (a)(1). OMB must also provide an update to the list of agency exceptions required in subsection (a)(2).

Section 109. Data and logging retention for incident response

Subsection (a) requires OMB, as determined appropriate by the Director of OMB and in consultation with NCD and the Director of CISA to update guidance for agencies regarding requirement for logging, log retention, log management, sharing of log data, and any other appropriate logging activity, within 2 years after the enactment of this Act.

Subsection (b) requires the Secretary of Defense to issue guidance that meets the standards required under subsection (a) for National Security Systems.

Section 110. CISA agency liaisons

This section creates a liaison between CISA and each agency. Within 120 days after enactment of FISMA 2023, CISA will assign each agency one CISA employee to be the liaison of that agency and CISA. This will clarify CISA's role, responsibility or services for that agency. This will also help CISA understand agency nuances to provide more custom cybersecurity guidance. This section specifies the qualification and duties of a liaison, and stipulates that the liaison shall not be a contractor but may be assigned to multiple senior agency information security officers. This section also directs CISA to consult with OMB to determine the duties of CISA liaisons to ensure these is no inappropriate duplication of activities. It also implements a rule of construction stating that nothing in this section will be construed to impact the ability of OMB to support agency implementation of federal cybersecurity requirements.

Section 111. Federal penetration testing policy

Subsection (a) amends 44 U.S.C. chapter 35 by adding section 3559A, which requires OMB to consult with CISA and issue guidance for agencies on penetration testing of information systems. It also requires OMB to provide policies governing the development of rules of engagement and procedures. Plans and guidelines on how to operate the penetration test will be developed within the agencies. Agencies are also expected to conduct their own penetration test on high value assets or coordinate with CISA to ensure that such testing is being performed. CISA will also establish processes to assess the performance of the penetration testing by both Federal and non-Federal entities; develop operational guidance for instituting penetration programs; develop and maintain capability to offer penetration testing as a service for Federal and non-Federal entities; and provide guidance to agencies on the best use of penetration testing resources. There is also an exception to this section for national security systems.

Section 112. Vulnerability disclosure policies

This section amends Title 44 by adding a new section, 3559B, which largely codifies existing OMB policy on vulnerability disclosure programs. This section requires that agencies create and follow a publicly available vulnerability disclosure policy. CISA is directed to support agencies in developing these tools and processes, as well as disclosing newly discovered vulnerabilities when requested. Additionally, OMB and agency heads may not publish information that would disrupt a law-enforcement, national security, intelligence, or national defense activity. This section does not apply to National Security Systems.

This section also moves several provisions from the Internet of Things Cybersecurity Improvement Act of 2020 into title 44, without amendment, to better organize existing law.

Section 113. Implementing zero trust architecture

This section requires OMB to provide a briefing within 1 year and a progress report submitted alongside the report required by Section 3553(c) of Title 44 during the 2–6 years following the enactment of this Act regarding agency progress in increasing the internal defenses of agency systems and on agency implementation of zero trust architectures. Additionally, the Secretary of Defense is directed to provide a briefing and progress reports under the same timeline to relevant congressional committees.

Section 114. Automation and artificial intelligence

This section requires OMB to issue guidance on the use of artificial intelligence (AI) by agencies to improve the cybersecurity of information systems, considering using AI wherever automation is currently used. The Director is required to report to relevant congressional committees detailing the use of automation and machine readable data across the Government for cybersecurity within 1 year of enactment and annually for 5 years thereafter.

Additionally, the Comptroller General is directed to submit two reports to relevant congressional committees. First, a report discussing the risks to individual privacy and the cybersecurity of information systems posed by Government use of artificial intelligence within 2 years of enactment. Second, a study on the use of automation, including artificial intelligence, and machine-readable data across the Government for cybersecurity purposes within 2 years of enactment.

Section 115. Extension of Chief Data Officer Council

This section extends the authorization for the Chief Data Officer Council until December 31, 2031.

Section 116. Council of the Inspectors General on integrity and efficiency dashboard

This section requires the Council of Inspectors General to create a dashboard, located on Oversight.gov, containing open information security recommendations identified in the evaluations required by 44 U.S.C. § 3555(a). It also makes clear that information exempted from disclosure under FOIA does not need to be included on the dashboard.

Section 117. Security operations center shared service

This section directs CISA to report to Congress their capabilities to create and operate a security operation center on behalf of other agencies.

Subsection (a) requires CISA to report to appropriate congressional Committees not later than 180 days after the enactment of this act, the existing shared cybersecurity services, the ability of these services to provide support to multiple agencies and integrate with other federal cybersecurity activities, and plans for expansion of shared cybersecurity services.

Subsection (b) requires a GAO report to be submitted to appropriate congressional Committees that identifies best practices for Federal cybersecurity security operations centers and recommendations for CISA to improve shared cybersecurity services.

Section 118. Federal cybersecurity requirements

This section moves, largely without alteration, language from existing FISMA 2014 law that is not in U.S. Code, into U.S. Code so it is more easily identifiable. This section changes existing law by adding a duration on existing agency exemption process for certain cybersecurity requirements, with congressional notification on any exemptions/extensions. It also adds a clarifying rule of construction regarding commercial product use by agencies to meet the requirements.

This section also moves certain provisions from the Internet of Things Cybersecurity Improvement Act of 2020 into Title 44, without amendment, to better organize existing law.

Section 119. Federal Chief Information Security Officer

This section establishes the position of a Presidentially appointed Chief Information Security Officer within OMB, reporting to the Federal Information Security Officer. The duties for this position are to carry out the information security functions within FISMA, the E Government Act of 2002, and other statutes, as well as Federal cybersecurity initiatives determined by the Chief Information Officer and specific electronic government initiatives currently authorized to the Director of OMB. Additionally, this section permits the individual serving as the Federal Chief Information Security Officer at enactment to continue to serve in this role without additional appointment.

Section 120. Renaming Office of the Federal Chief Information Officer

This section renames relevant parts of the U.S. Code in accordance with the changes made by this Act. Additionally, the individual serving as the Administrator of the Office of Electronic Government at enactment may continue to serve as the Federal Chief Information Officer without additional appointment.

Section 121. Rules of construction

This section clarifies that nothing in this title may be used to authorize an agency to take an action not authorized by law, nor may it be used to violate the constitutionally protected rights of any individual. This section also clarifies that nothing in this title may

be construed to impinge on the privacy rights of individuals or allow the unauthorized access, sharing, or use of personal data.

TITLE II—RURAL HOSPITAL CYBERSECURITY ENHANCEMENT ACT

Section 201. Short title

This section designates title II as the "Rural Hospital Cybersecurity Enhancement Act."

Section 202. Definitions

This section defines the terms "agency," "appropriate committees of Congress," "Director," "geographic division," "rural hospital," and "Secretary."

Section 203. Rural hospital cybersecurity workforce development strategy

Subsection (a) requires the Secretary of Homeland Security, acting through the Director of CISA, to develop and transmit a comprehensive rural hospital cybersecurity workforce development strategy to the Senate Homeland Security and Governmental Affairs Committee (HSGAC) and the House Committee on Homeland Security (CHS).

Subsection (b) allows the Secretary of Homeland Security and CISA Director to consult with the Secretaries of Health and Human Services, Education, Labor, and any other appropriate agency in carrying out subsection (a). It also requires the Secretary of Homeland Security to consult with at least two representatives of rural healthcare providers from each of the nine U.S. geographic divisions determined by the Census Bureau.

Subsection (c) requires that the strategy under subsection (a) consider partnerships with non-governmental entities, cybersecurity curricula and teaching resources for use in rural educational institutions, identification of and best practices to mitigate cybersecurity workforce challenges in rural hospitals, and policy recommendations.

Subsection (d) requires the Secretary of Homeland Security to provide an annual briefing to HSGAC and CHS that includes updates to the strategy, any programs or initiatives established pursuant to the strategy and the number of individuals served, additional policy recommendations, and the effectiveness of the strategy in addressing the need for skilled cybersecurity professionals in rural hospitals.

Section 204. Instructional materials for rural hospitals

Subsection (a) requires the CISA Director to make available instructional materials for rural hospitals that can be used to train staff on fundamental cybersecurity efforts.

Subsection (b) requires the CISA Director to, in carrying out subsection (a), consult with appropriate federal agencies and non-governmental experts, identify existing materials that can be adapted for use and create new materials as needed, and conduct an awareness campaign to promote the materials.

Section 205. No additional funds

This section states that no additional funds are authorized to be appropriated for the purpose of carrying out this bill.

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

At a Glance

S. 2251, Cybersecurity Act of 2023

As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on July 26, 2023

By Fiscal Year, Millions of Dollars	2023	2023-2028	2023-2033
Direct Spending (Outlays)	0	*	*
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	*	*
Spending Subject to Appropriation (Outlays)	0	735	not estimated

Increases *net direct spending* in any of the four consecutive 10-year periods beginning in 2034?	< $2.5 billion	Statutory pay-as-you-go procedures apply?	Yes
		Mandate Effects	
Increases *on-budget deficits* in any of the four consecutive 10-year periods beginning in 2034?	< $5 billion	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

* = between zero and $500,000.

The bill would:

- Update policies, procedures, and programs for information security at federal agencies
- Require all federal agencies to report significant cyber incidents on their networks
- Codify the responsibilities of the federal Chief Information Security Officer
- Direct the Cybersecurity and Infrastructure Security Agency to study cyber threats to rural hospitals

Estimated budgetary effects would mainly stem from:

- Reporting and responding to cyber incidents at federal agencies
- Contracting with information security service companies
- Providing cyber incident response training to federal employees
- Hiring information security analysts

• Developing training resources for rural hospital employees

Areas of significant uncertainty include:

• Anticipating the adoption schedules of new cybersecurity procedures and programs

• Predicting the staffing and contracting requirements of federal information security offices

Bill summary: The Federal Information Security Modernization Act (FISMA) provides a framework to protect government information operations against cybersecurity threats. S. 2251 would update FISMA to require federal agencies to report all cybersecurity incidents and conduct standardized cybersecurity procedures on a regular basis.

S. 2251 also would require the Cybersecurity and Infrastructure Security Agency (CISA) to study cybersecurity threats facing rural hospitals. Under the bill, CISA would provide the Congress with recommendations to improve the recruitment and training of cyber professionals at rural hospitals. The bill also would require CISA to develop and disseminate information on cyber safety measures to employees of rural hospitals.

Estimated Federal cost: The estimated budgetary effects of S. 2251 are shown in Table 1. The costs of the legislation fall within budget functions 050 (national defense) and 800 (general government).

TABLE 1.—ESTIMATED BUDGETARY EFFECTS OF S. 2251

	By fiscal year, millions of dollars—						
	2023	2024	2025	2026	2027	2028	2023–2028
Federal Information Security Modernization:							
Estimated Authorization	0	75	125	175	225	230	830
Estimated Outlays	0	44	103	153	203	227	730
Rural Hospital Cybersecurity:							
Estimated Authorization	0	1	1	1	1	1	5
Estimated Outlays	0	1	1	1	1	1	5
Total Changes:							
Estimated Authorization	0	76	126	176	226	231	835
Estimated Outlays	0	5	104	154	204	228	735

In addition to the budgetary effects shown above, CBO estimates that enacting S. 2251 would have insignificant effects on direct spending and the deficit over the 2023–2033 period.

Basis of estimate: For this estimate, CBO assumes that S. 2251 will be enacted early in fiscal year 2024. Outlays are based on historical spending patterns for existing or similar programs.

Spending subject to appropriation: CBO estimates that implementing the bill would cost $735 million over the 2023–2028 period. Such spending would be subject to the availability of appropriated funds.

Federal Information Security Modernization. Most of the provisions of S. 2251 would codify or expand current practices of the federal government. FISMA established regulations and guidelines for ensuring the effectiveness of security controls over information resources that support federal information security operations and assets. Specifically, FISMA requires the head of each agency to provide information security protections commensurate with the risk and magnitude of harm that would result from the unauthorized access, use, disclosure, disruption, modification, or destruction of

information and information systems used or operated by each agency. The Office of Management and Budget (OMB) and the Cybersecurity and Infrastructure Security Agency develop policies, measures, standards, and guidelines for these purposes. Inspectors general perform independent evaluations of the information security programs and practices of individual agencies. Federal civilian agencies spent more than $10 billion on cybersecurity activities in fiscal year 2022.

CBO expects that implementing S. 2251 would require agencies to perform additional cybersecurity procedures to identify weaknesses in federal networks and report security incidents to CISA. CBO anticipates that agencies would hire additional personnel and contract with third-party entities to implement new data management and reporting requirements under S. 2251. Based on information from OMB and other agencies about the costs to administer similar policies, CBO estimates that the new and expanded activities under the legislation would increase current civilian cybersecurity expenses by 2 percent, or about $225 million annually when fully implemented. CBO expects that it would take about four years to reach that level of effort for the roughly 10,000 federal computer systems currently operating. CBO estimates that implementing those new requirements would increase costs by $44 million in 2024 and $730 million over the 2023–2028 period.

Rural Hospital Cybersecurity. Using information from CISA about studies, information sharing, and training efforts similar to those that the bill would require for rural hospitals, CBO anticipates that the agency would need two full-time employees to prepare the reports and to develop online training resources for rural hospital employees. CBO estimates that staff salaries and technology costs to publish instructional materials would total $5 million over the 2023–2028 period.

Direct Spending: Enacting the bill could affect direct spending by some federal agencies that are allowed to use fees, receipts from the sale of goods, and other collections to cover operating costs. CBO estimates that any net changes in direct spending by those agencies would be negligible because most of them can adjust amounts collected to reflect changes in operating costs.

Uncertainty: Areas of uncertainty in this estimate include predicting the implementation timeline at federal agencies. The budgetary effects of the bill could be significantly higher or lower than CBO's estimate if the time needed to adopt new cybersecurity procedures and technology differs from CBO's estimate.

The budgetary effects of the bill also would depend on the number of additional employees that would be needed at OMB, CISA, and other federal agencies to satisfy the requirements of the bill. Costs would be moderately larger or smaller than this estimate depending on how the number of software analysts hired differs from CBO's estimate.

Pay-As-You-Go considerations: The Statutory Pay-As-You-Go Act of 2010 establishes budget-reporting and enforcement procedures for legislation affecting direct spending or revenues. CBO estimates that enacting the bill would increase direct spending by less than $500,000 over the 2023–2033 period.

Increase in long-term net direct spending and deficits: CBO estimates that enacting S. 2251 would not significantly increase net di-

rect spending in any of the four consecutive 10-year periods beginning in 2034.

CBO estimates that enacting S. 2251 would not significantly increase on-budget deficits in any of the four consecutive 10-year periods beginning in 2034.

Mandates: None.

Previous CBO estimate: On June 23, 2023, CBO transmitted a cost estimate for S. 1560, the Rural Hospital Cybersecurity Enhancement Act, as ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on June 14, 2023. Title II of S. 2251 is similar to S. 1560 and CBO's estimates of their budgetary effects are the same.

Estimate prepared by: Federal Costs: Aldo Prosperi. Mandates: Brandon Lever.

Estimate reviewed by: David Newman, Chief, Defense, International Affairs, and Veterans' Affairs Cost Estimates Unit; Kathleen FitzGerald, Chief, Public and Private Mandates Unit; Christina Hawley Anthony, Deputy Director of Budget Analysis.

Estimate approved by: Phillip L. Swagel, Director, Congressional Budget Office.

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 the bill, 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):

UNITED STATES CODE

* * * * * * *

TITLE 5—GOVERNMENT ORGANIZATION AND EMPLOYEES

* * * * * * *

PART 1—THE AGENCIES GENERALLY

* * * * * * *

CHAPTER 4—INSPECTORS GENERAL

* * * * * * *

SEC. 424. ESTABLISHMENT OF THE COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY.

(a) * * *

* * * * * * *

(e) * * *

(1) * * *

(2) * * *

(A) to consolidate all public reports from each Office of Inspector General to improve the access of the public to

any audit report, inspection report, or evaluation report (or portion of any such report) made by an Office of Inspector General; [and]

(B) that shall include a dashboard of open information security recommendations identified in the independent evaluations required by section 3555(a) of title 44; and

[(B)]*(C)* that shall include any additional resources, information, and enhancements as the Council determines are necessary or desirable.

(3) * * *

(4) * * *

(5) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to require the publication of information that is exempted from disclosure under section 552 of this title.

* * * * * * *

CHAPTER 5—ADMINISTRATIVE PROCEDURE

* * * * * * *

Subchapter II—Administrative Procedure

* * * * * * *

SEC. 552a. RECORDS MAINTAINED ON INDIVIDUALS.

(a) * * *

(b) * * *

(1) * * *

* * * * * * *

(11) pursuant to the order of a court of competent jurisdiction; [or]

(12) to a consumer reporting agency in accordance with section 3711(e) of title 31[.]*; or*

(13) to another agency, to the extent necessary, to assist the recipient agency in responding to an incident (as defined in section 3552 of title 44) or breach (as defined in section 3591 of title 44) or to fulfill the information sharing requirements under section 3594 of title 44.

* * * * * * *

TITLE 10—ARMED FORCES

* * * * * * *

Subtitle A—General—Military Law

* * * * * * *

PART IV—SERVICE, SUPPLY, AND PROPERTY

* * * * * * *

CHAPTER 131—PLANNING AND COORDINATION

* * * * * * *

SEC. 2222. DEFENSE BUSINESS SYSTEMS: BUSINESS PROCESS RE-ENGINEERING; ENTERPRISE ARCHITECTURE; AND MANAGEMENT.

(a) * * *

* * * * * * *

(i) * * *

(1) * * *

* * * * * * *

(6) ENTERPRISE ARCHITECTURE.—The term "enterprise architecture" has the meaning given that term in [section 3601(4)] *section 3601* of title 44.

* * * * * * *

(8) NATIONAL SECURITY SYSTEM.—The term "national security system" has the meaning given that term in [section 3552(b)(6)(A)] *section 3552(b)(8)(A)* of title 44.

* * * * * * *

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

* * * * * * *

(c) * * *

(1) * * *

(2) * * *

(3) The term "national security system" has the meaning given that term by [section 3552(b)(6)] *section 3552(b)* of title 44.

* * * * * * *

PART V—ACQUISITION

* * * * * * *

Subpart A—General

* * * * * * *

CHAPTER 203—GENERAL MATTERS

* * * * * * *

SEC. 3068. INAPPLICABILITY OF CERTAIN LAWS.

(a) * * *

(b) LAWS INAPPLICABLE TO 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 3552(b)(6)] *section 3552(b)* of title 44.

* * * * * * *

Subpart B—Acquisition Planning

* * * * * * *

CHAPTER 223—OTHER PROVISIONS RELATING TO PLANNING AND SOLICITATION GENERALLY

* * * * * * *

SEC. 3252. REQUIREMENTS FOR INFORMATION RELATING TO SUPPLY CHAIN RISK.

* * * * * * *

(e) * * *

* * * * * * *

(5) COVERED SYSTEM.—The term "covered system" means a national security system, as that term is defined in [section 3552(b)(6)] *section 3552(b)* of title 44.

* * * * * * *

TITLE 40—PUBLIC BUILDINGS, PROPERTY, AND WORKS

* * * * * * *

Subtitle III—Information Technology Management

* * * * * * *

CHAPTER 113—RESPONSIBILITY FOR ACQUISITIONS OF INFORMATION TECHNOLOGY

* * * * * * *

Subchapter I—Director of Office of Management and Budget

* * * * * * *

SEC. 11302. CAPITAL PLANNING AND INVESTMENT CONTROL.

(a) * * *

(b) USE OF INFORMATION TECHNOLOGY IN FEDERAL PROGRAMS.—The Director shall promote and improve the acquisition, [use, security, and disposal of] *use, and disposal of, and, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director, promote and improve the security of,* information technology by the Federal government to improve the productivity, efficiency, and effectiveness of federal programs, including through dissemination of public information and the reduction of information collection burdens on the public.

* * * * * * *

(h) COMPARISON OF AGENCY USES OF INFORMATION TECHNOLOGY.—The Director shall compare the performances, *including cybersecurity performances,* of the executive agencies in using information technology and shall disseminate the comparisons to the heads of the executive agencies.

* * * * * * *

SEC. 11303. PERFORMANCE-BASED AND RESULTS-BASED MANAGEMENT.

(a) * * *
(b) * * *
(1) * * *
(2) * * *
(A) * * *
(B) * * *

(i) whether the function to be supported by the system should be performed by the private sector and, if so, whether any component of the executive agency performing that function should be converted from a governmental organization to a private sector organization; **[**or**]**

(ii) whether the function should be performed by the executive agency and, if so, whether the function should be performed by a private sector source under contract or by executive agency personnel; *or*

(iii) whether the function should be performed by a shared service offered by another executive agency;

* * * * * * *

Subchapter II—Executive Agencies

* * * * * * *

SEC. 11312. CAPITAL PLANNING AND INVESTMENT CONTROL.

(a) DESIGN OF PROCESS.—In fulfilling the responsibilities assigned under section 3506(h) of title 44, the head of each executive agency shall design and implement in the executive agency a process for maximizing the value, and assessing and managing the risks, *including security risks*, of the information technology acquisitions of the executive agency.

* * * * * * *

SEC. 11313. PERFORMANCE AND RESULTS-BASED MANAGEMENT.

In fulfilling the responsibilities undersection 3506(h) of title 44, the head of an executive agency shall—

(1) establish goals for improving the **[**efficiency and effectiveness**]** *efficiency, security, and effectiveness* of agency operations and, as appropriate, the delivery of services to the public through the effective use of information technology;

* * * * * * *

SEC. 11317. SIGNIFICANT DEVIATIONS.

The head of each executive agency shall identify in the strategic information resources management plan required under section 3506(b)(2) of title 44 any major information technology acquisition program, or any phase or increment of that program, that has significantly deviated from the cost, performance, *security*, or schedule goals established for the program.

* * * * * * *

SEC. 11319. RESOURCES, PLANNING, AND PORTFOLIO MANAGEMENT.

(a) * * *
(b) * * *

(1) PLANNING, PROGRAMMING, BUDGETING, AND EXECUTION AUTHORITIES FOR [CIOS] *CHIEF INFORMATION OFFICERS.*—

* * * * * * *

TITLE 44—PUBLIC PRINTING AND DOCUMENTS

* * * * * * *

CHAPTER 35—COORDINATION OF FEDERAL INFORMATION POLICY

Table of sections

* * * * * * *

Subchapter I—Federal Information Policy

* * * * * * *

SEC. 3504. AUTHORITY AND FUNCTIONS OF DIRECTOR.

(a) * * *

(1) * * *

(A) * * *

(B) * * *

(i) * * *

* * * * * * *

[(v) privacy, confidentiality, security, disclosure, and sharing of information; and]

(v) privacy, confidentiality, disclosure, and sharing of information;

(vi) in consultation with the National Cyber Director, security of information; and

[(vi)]*(vii)* * * *

* * * * * * *

(g) * * *

[(1) develop and oversee the implementation of policies, principles, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for agencies; and]

(1) develop and oversee the implementation of policies, principles, standards, and guidelines on privacy, confidentiality, disclosure, and sharing of information collected or maintained by or for agencies;

(2) in consultation with the National Cyber Director, oversee the implementation of policies, principles, standards, and guidelines on security, of information collected or maintained by or for agencies; and

[(2)]*(3)* * * *

* * * * * * *

SEC. 3505. ASSIGNMENT OF TASKS AND DEADLINES.

(a) * * *

* * * * * * *

[(c) INVENTORY OF MAJOR INFORMATION SYSTEMS.—(1) The head of each agency shall develop and maintain an inventory of major information systems (including major national security systems) operated by or under the control of such agency.

[(2) The identification of information systems in an inventory under this subsection shall include an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.

[(3) Such inventory shall be—

[(A) updated at least annually;

[(B) made available to the Comptroller General; and

[(C) used to support information resources management, including—

[(i) preparation and maintenance of the inventory of information resources under section 3506(b)(4);

[(ii) information technology planning, budgeting, acquisition, and management under section 3506(h), subtitle III of title 40, and related laws and guidance;

[(iii) monitoring, testing, and evaluation of information security controls under subchapter II;

[(iv) preparation of the index of major information systems required under section 552(g) of title 5, United States Code; and

[(v) preparation of information system inventories required for records management under chapters 21, 29, 31, and 33.

[(4) The Director shall issue guidance for and oversee the implementation of the requirements of this subsection.]

(c) INVENTORY OF INFORMATION SYSTEMS.

(1) * * *

(2) The identification of information systems in an inventory under this subsection shall include *an identification of internet accessible information systems and* an identification of the interfaces between each such system and all other systems or

networks, including those not operated by or under the control of the agency;

(3) Such inventory shall be—

(A) * * *

(B) made available to *the Director of the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, and* the Comptroller General; [and]

(C) * * *

(i) * * *

* * * * * * *

(v) preparation of information system inventories required for records management under chapters 21, 29, 31, and 33[.] *; and*

(D) maintained on a continual basis through the use of automation, machine-readable data, and scanning, wherever practicable.

* * * * * * *

SEC. 3506. FEDERAL AGENCY RESPONSIBILITIES.

(a) * * *

(1) * * *

(2) * * *

(3) The Chief Information Officer designated under paragraph (2) shall head an office responsible for ensuring agency compliance with and prompt, efficient, and effective implementation of the information policies and information resources management responsibilities established under this subchapter, including the reduction of information collection burdens on the public. *In carrying out these duties, the Chief Information Officer shall consult, as appropriate, with the Chief Data Officer in accordance with the designated functions under section 3520(c).* The Chief Information Officer and employees of such office shall be selected with special attention to the professional qualifications required to administer the functions described under this subchapter.

(b) * * *

(1) * * *

(A) * * *

(B) * * *

(C) improve the integrity, *availability*, quality, and utility of information to all users within and outside the agency, including capabilities for ensuring dissemination of public information, public access to government information, and protections for privacy and security;

* * * * * * *

(h) * * *

(1) * * *

(2) * * *

(3) promote the use of information technology by the agency to improve the productivity, efficiency, *security*, and effectiveness of agency programs, including the reduction of information collection burdens on the public and improved dissemination of public information;

* * * * * * *

(j)(1) Nothwithstanding paragraphs (2) and (3) of subsection (a), the head of each agency shall, in accordance with section 552(a) of division H of the Consolidated Appropriations Act, 2005 (42 U.S.C. 2000ee–2), designate a Chief Privacy Officer with the necessary skills, knowledge, and expertise, who shall have the authority and responsibility to—

(A) lead the privacy program of the agency; and

(B) carry out the privacy responsibilities of the agency under this chapter, section 552a of title 5, and guidance issued by the Director.

(2) The Chief Privacy Officer of each agency shall—

(A) serve in a central leadership position within the agency;

(B) have visibility into relevant agency operations; and

(C) be positioned highly enough within the agency to regularly engage with other agency leaders and officials, including the head of the agency.

(3) A privacy officer of an agency established under a statute enacted before the date of enactment of the Federal Information Security Modernization Act of 2023 may carry out the responsibilities under this subsection for the agency.

* * * * * * *

SEC. 3513. DIRECTOR REVIEW OF AGENCY ACTIVITIES; REPORTING; AGENCY RESPONSE.

(a) * * *

(b) * * *

(c) Each agency providing a written plan under subsection (b) shall provide any portion of the written plan addressing information security to the Secretary of Homeland Security and the National Cyber Director.

[(c)**]***(d)* * * *

* * * * * * *

SEC. 3520A. CHIEF DATA OFFICER COUNCIL.

(a) * * *

* * * * * * *

(e) * * *

(1) * * *

(2) TERMINATION OF COUNCIL.—The Council shall terminate and this section shall be repealed **[**upon the expiration of the 2-year period that begins on the date the Comptroller General submits the report under paragraph (1) to Congress**]** *December 31, 2031.*

* * * * * * *

SUBCHAPTER II—INFORMATION SECURITY

SEC. 3551. PURPOSES.

The purposes of this subchapter are to—

(1) * * *

(2) * * *

(3) * * *

(4) provide a mechanism for improved oversight of Federal agency information security programs, including through auto-

mated security tools to continuously [diagnose and improve] *integrate, deliver, diagnose, and improve* security;

(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[.] *;*

(7) recognize that each agency has specific mission requirements and, at times, unique cybersecurity requirements to meet the mission of the agency;

(8) recognize that each agency does not have the same resources to secure agency systems, and an agency should not be expected to have the capability to secure the systems of the agency from advanced adversaries alone; and

(9) recognize that a holistic Federal cybersecurity model is necessary to account for differences between the missions and capabilities of agencies.

* * * * * * *

SEC. 3552. DEFINITIONS.

(a) * * *

(b) * * *

(1) * * *

(2) The term 'high value asset' means information or an information system that the head of an agency, using policies, principles, standards, or guidelines issued by the Director under section 3553(a), determines to be so critical to the agency that the loss or degradation of the confidentiality, integrity, or availability of such information or information system would have a serious impact on the ability of the agency to perform the mission of the agency or conduct business.

[(2)]*(3)* * * *

[(3)]*(4)* * * *

[(4)]*(5)* * * *

[(5)]*(6)* * * *

(7) The term 'major incident' has the meaning given the term in guidance issued by the Director under section 3598(a).

[(6)]*(8)*(A) The term "national security system" means any information system (including any telecommunications system) [used] *owned, managed,* or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

(i) * * *

(ii) * * *

(B) * * *

(9) The term 'penetration test'—

(A) means an authorized assessment that emulates attempts to gain unauthorized access to, or disrupt the oper-

ations of, an information system or component of an information system; and

(B) includes any additional meaning given the term in policies, principles, standards, or guidelines issued by the Director under section 3553(a).

[(7)**]***(10)* * * *

(11) The term 'shared service' means a centralized mission capability or consolidated business function that is provided to multiple organizations within an agency or to multiple agencies.

(12) The term 'zero trust architecture' has the meaning given the term in Special Publication 800–207 of the National Institute of Standards and Technology, or any successor document.

* * * * * * *

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

(a) * * *

(1) * * *

* * * * * * *

(5) overseeing agency compliance with the requirements of this subchapter andsection 1326 of title 41, including through any authorized action undersection 11303 of title 40, to enforce accountability for compliance with such requirements; **[**and**]**

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

(7) promoting, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, and the Director of the National Institute of Standards and Technology—

(A) the use of automation to improve Federal cybersecurity and visibility with respect to the implementation of Federal cybersecurity; and

(B) the use of presumption of compromise and least privilege principles, such as zero trust architecture, to improve resiliency and timely response actions to incidents on Federal systems.

(b) SECRETARY.—The Secretary, in consultation with the Director *and the National Cyber Director*, shall administer the implementation 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) * * *

(2) * * *

(A) requirements for reporting security incidents to the Federal information security incident center established under section 3556 *and reporting requirements under subchapter IV of this chapter*;

* * * * * * *

(7) * * *

(8) expeditiously seeking opportunities to reduce costs, administrative burdens, and other barriers to information technology

security and modernization for agencies, including through shared services for cybersecurity capabilities identified as appropriate by the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and other agencies as appropriate;

(9) performing penetration testing that may leverage manual expert analysis to identify threats and vulnerabilities within information systems—

(A) without consent or authorization from agencies; and

(B) with prior notification to the head of the agency;

[(8)**]***(10)* * * *

[(9)**]***(11)* * * *

(c) REPORT.—Not later than March 1 of **[**each year**]** *each year during which agencies are required to submit reports under section 3554(c)*, the Director, in consultation with the Secretary, shall submit to Congress a report, *which shall be unclassified but may include 1 or more annexes that contain classified or other sensitive information, as appropriate* on the effectiveness of information security policies and practices during the **[**preceding year**]** *preceding 2 years*, 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)**]***(1)* * * *

[(3)**]***(2)* * * *

[(4)**]***(3)* an assessment of agency compliance with standards promulgated undersection 11331 of title 40; **[**and**]**

(4) a summary of the risks and trends identified in the Federal risk assessment required under subsection (i); and

* * * * * * *

(h) DIRECTION TO AGENCIES.—

(1) * * *

(A) * * *

(B) * * *

(2) * * *

(A) in coordination with the Director *and the National Cyber Director*, and in consultation with Federal contractors as appropriate, establish procedures governing the circumstances under which a directive may be issued under this subsection, which shall include—

* * * * * * *

(D) notify the Director, *the National Cyber Director*, and the head of any affected agency immediately upon the issuance of a directive under this subsection;

* * * * * * *

(3) IMMINENT THREATS.—

(A) * * *

(i) * * *

(ii) * * *

(iii) * * *

(iv) the Secretary provides prior notice to the Director, *the National Cyber Director*, and the head and chief information of-

ficer (or equivalent official) of each agency to which specific actions will be taken pursuant to this paragraph, and notifies the appropriate congressional committees and authorizing committees of each such agency within 7 days of taking an action under this paragraph of—

* * * * * * *

[(i) ANNUAL REPORT TO CONGRESS.—Not later than February 1 of each year, the Director and the Secretary shall submit to the appropriate congressional committees a report regarding the specific actions the Director and the Secretary have taken pursuant to subsection (a)(5), including any actions taken pursuant to section 11303(b)(5) of title 40.]

(i) FEDERAL RISK ASSESSMENT.—On an ongoing and continuous basis, the Director of the Cybersecurity and Infrastructure Security Agency shall assess the Federal risk posture using any available information on the cybersecurity posture of agencies, and brief the Director and National Cyber Director on the findings of such assessment, including—

(1) the status of agency cybersecurity remedial actions for high value assets described in section 3554(b)(7);

(2) any vulnerability information relating to the systems of an agency that is known by the agency;

(3) analysis of incident information under section 3597;

(4) evaluation of penetration testing performed under section 3559A;

(5) evaluation of vulnerability disclosure program information under section 3559B;

(6) evaluation of agency threat hunting results;

(7) evaluation of Federal and non-Federal cyber threat intelligence;

(8) data on agency compliance with standards issued under section 11331 of title 40;

(9) agency system risk assessments required under section 3554(a)(1)(A);

(10) relevant reports from inspectors general of agencies and the Government Accountability Office; and

(11) any other information the Director of the Cybersecurity and Infrastructure Security Agency determines relevant.

* * * * * * *

(m) DIRECTIVES.—

(1) EMERGENCY DIRECTIVE UPDATES.—If the Secretary issues an emergency directive under this section, the Director of the Cybersecurity and Infrastructure Security Agency shall submit to the Director, the National Cyber Director, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committees on Oversight and Accountability and Homeland Security of the House of Representatives an update on the status of the implementation of the emergency directive at agencies not later than 7 days after the date on which the emergency directive requires an agency to complete a requirement specified by the emergency directive, and every 30 days thereafter until—

(A) the date on which every agency has fully implemented the emergency directive;

(B) the Secretary determines that an emergency directive no longer requires active reporting from agencies or additional implementation; or

(C) the date that is 1 year after the issuance of the directive.

(2) BINDING OPERATIONAL DIRECTIVE UPDATES.—If the Secretary issues a binding operational directive under this section, the Director of the Cybersecurity and Infrastructure Security Agency shall submit to the Director, the National Cyber Director, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committees on Oversight and Accountability and Homeland Security of the House of Representatives an update on the status of the implementation of the binding operational directive at agencies not later than 30 days after the issuance of the binding operational directive, and every 90 days thereafter until—

(A) the date on which every agency has fully implemented the binding operational directive;

(B) the Secretary determines that a binding operational directive no longer requires active reporting from agencies or additional implementation; or

(C) the date that is 1 year after the issuance or substantive update of the directive.

(3) REPORT.—If the Director of the Cybersecurity and Infrastructure Security Agency ceases submitting updates required under paragraphs (1) or (2) on the date described in paragraph (1)(C) or (2)(C), the Director of the Cybersecurity and Infrastructure Security Agency shall submit to the Director, the National Cyber Director, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committees on Oversight and Accountability and Homeland Security of the House of Representatives a list of every agency that, at the time of the report—

(A) has not completed a requirement specified by an emergency directive; or

(B) has not implemented a binding operational directive.

(n) REVIEW OF OFFICE OF MANAGEMENT AND BUDGET GUIDANCE AND POLICY.—

(1) CONDUCT OF REVIEW.—Not less frequently than once every 3 years, the Director of the Office of Management and Budget shall review the efficacy of the guidance and policy promulgated by the Director in reducing cybersecurity risks, including a consideration of reporting and compliance burden on agencies.

(2) CONGRESSIONAL NOTIFICATION.—The Director of the Office of Management and Budget shall notify the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Accountability of the House of Representatives of changes to guidance or policy resulting from the review under paragraph (1).

(3) GAO REVIEW.—The Government Accountability Office shall review guidance and policy promulgated by the Director to assess its efficacy in risk reduction and burden on agencies.

(o) AUTOMATED STANDARD IMPLEMENTATION VERIFICATION.—When the Director of the National Institute of Standards and Technology issues a proposed standard or guideline pursuant to para-

graphs (2) or (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)), the Director of the National Institute of Standards and Technology shall consider developing and, if appropriate and practical, develop specifications to enable the automated verification of the implementation of the controls.

(p) INSPECTORS GENERAL ACCESS TO FEDERAL RISK ASSESSMENTS.—The Director of the Cybersecurity and Infrastructure Security Agency shall, upon request, make available Federal risk assessment information under subsection (i) to the Inspector General of the Department of Homeland Security and the inspector general of any agency that was included in the Federal risk assessment.

* * * * * * *

SEC. 3554. FEDERAL AGENCY RESPONSIBILITIES.

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

(1) be responsible for—

(A) on an ongoing and continuous basis, assessing agency system risk, as applicable, by—

(i) identifying and documenting the high value assets of the agency using guidance from the Director;

(ii) evaluating the data assets inventoried under section 3511 for sensitivity to compromises in confidentiality, integrity, and availability;

(iii) identifying whether the agency is participating in federally offered cybersecurity shared services programs;

(iv) identifying agency systems that have access to or hold the data assets inventoried under section 3511;

(v) evaluating the threats facing agency systems and data, including high value assets, based on Federal and non-Federal cyber threat intelligence products, where available;

(vi) evaluating the vulnerability of agency systems and data, including high value assets, including by analyzing—

(I) the results of penetration testing performed by the Department of Homeland Security under section 3553(b)(9);

(II) the results of penetration testing performed under section 3559A;

(III) information provided to the agency through the vulnerability disclosure program of the agency under section 3559B;

(IV) incidents; and

(V) any other vulnerability information relating to agency systems that is known to the agency;

(vii) assessing the impacts of potential agency incidents to agency systems, data, and operations based on the evaluations described in clauses (ii) and (v) and the agency systems identified under clause (iv); and

(viii) assessing the consequences of potential incidents occurring on agency systems that would impact systems at other agencies, including due to interconnectivity between different agency systems or

operational reliance on the operations of the system or data in the system;

[(A)]*(B)* [providing information] *using information from the assessment required under subparagraph (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) * * *

(ii) * * *

[(B)]*(C)* complying with the requirements of this subchapter, subchapter III of chapter 13 of title 41, and related policies, procedures, standards, and guidelines, including—

(i) * * *

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

(iii) * * *

(iv) * * *

(v) * * *

(vi) responsibilities relating to assessing and avoiding, mitigating, transferring, or accepting supply chain risks undersection 1326 of title 41, and complying with exclusion and removal orders issued under section 1323 of such title; [and]

[(C)]*(D)* * * *

(E) providing an update on the ongoing and continuous assessment required under subparagraph (A)—

(i) upon request, to the inspector general of the agency or the Comptroller General of the United States; and

(ii) at intervals determined by guidance issued by the Director, and to the extent appropriate and practicable using automation, to—

(I) the Director;

(II) the Director of the Cybersecurity and Infrastructure Security Agency; and

(III) the National Cyber Director;

(2) * * *

(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 *in accordance with the agency system risk assessment required under paragraph (1)(A);*

(B) * * *

(C) * * *

(D) periodically, *through the use of penetration testing, the vulnerability disclosure program established under section 3559B, and other means*, testing and evaluating information security controls and techniques to ensure that they are effectively implemented;

(3) * * *

(A) designating a [senior agency information security officer] *Chief Information Security Officer* who shall—

(i) carry out the Chief Information Officer's responsibilities under [this section] *subsections (a) through (c);*

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

(iii) *manage information security, cybersecurity budgets, and risk and compliance activities and explain those concepts to the head of the agency and the executive team of the agency;*

[(iii)]*(iv)* have [information security duties as that official's primary duty] *information, computer network, and technology security duties as the Chief Information Security Officers' primary duty; and*

[(iv)]*(v)* * * *

* * * * * * *

(5) ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports [annually] *not less frequently than quarterly* 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] *Chief Information Security Officer delegated* authority under paragraph (3); and

(7) * * *

(b) * * *

[(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, which may include using automated tools consistent with standards and guidelines promulgated under section 11331 of title 40;]

(1) the ongoing and continuous assessment of agency system risk required under subsection (a)(1)(A), which may include using guidance and automated tools consistent with standards and guidelines promulgated under section 11331 of title 40, as applicable;

(2) * * *

(A) * * *

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

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

[(D)]*(C)* * * *

(i) * * *

(ii) * * *

(iii) binding operational directives and emergency directives issued by the Secretary under section 3553;

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

determined by the agency, considering the agency risk assessment required under subsection (a)(1)(A);

[(iv)]*(v)* * * *

(3) * * *

(4) * * *

(5) * * *

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

(B) * * *

(C) * * *

(6) * * *

(7) a secure process for providing the status of every remedial action and unremediated identified system vulnerability of a high value asset to the Director and the Director of the Cybersecurity and Infrastructure Security Agency, using automation and machine-readable data to the greatest extent practicable;

[(7)]*(8)* * * *

(A) * * *

(B) * * *

(C) shall include—

(i) * * *

[(ii) notifying and consulting with the Federal information security incident center established in section 3556; and]

(ii) notifying and consulting with the Federal information security incident center established under section 3556 pursuant to the requirements of section 3594;

(iii) performing the notifications and other activities required under subchapter IV of this chapter; and

[(iii)](iv) * * *

(I) * * *

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

[(III) for a major incident, the committees of Congress described in subsection (c)(1)—

[(aa) not later than 7 days after the date on which there is a reasonable basis to conclude that the major incident has occurred; and

[(bb) after the initial notification under item (aa), within a reasonable period of time after additional information relating to the incident is discovered, including the summary required under subsection (c)(1)(A)(i); and]

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

[(8)]*(9)* * * *

(c) * * *

[(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 Af-

fairs 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;

[(III) the status of compliance of the affected information systems with applicable security requirements at the time of the incident; and

[(IV) 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, as defined by the Director, 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 Director or the Secretary, in consultation with the Director, 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).]

(1) BIENNIAL REPORT.—Not later than 2 years after the date of enactment of the Federal Information Security Modernization Act of 2023 and not less frequently than once every 2 years thereafter, using the continuous and ongoing agency system risk assessment required under subsection (a)(1)(A), the head of each agency shall submit to the Director, the National Cyber Director, the Director of the Cybersecurity and Infrastructure Security Agency, the Comptroller General of the United States, the

majority and minority leaders of the Senate, the Speaker and minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Accountability of the House of Representatives, the Committee on Homeland Security of the House of Representatives, the Committee on Commerce, Science, and Transportation of the Senate, the Committee on Science, Space, and Technology of the House of Representatives, and the appropriate authorization and appropriations committees of Congress a report that—

(A) summarizes the agency system risk assessment required under subsection (a)(1)(A);

(B) evaluates the adequacy and effectiveness of information security policies, procedures, and practices of the agency to address the risks identified in the agency system risk assessment required under subsection (a)(1)(A), including an analysis of the agency's cybersecurity and incident response capabilities using the metrics established under section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c));

(C) summarizes the status of remedial actions identified by inspector general of the agency, the Comptroller General of the United States, and any other source determined appropriate by the head of the agency; and

(D) with respect to any exemption from the requirements of subsection (f)(3) that is effective on the date of submission of the report, includes the number of information systems that have received an exemption from those requirements.

(2) UNCLASSIFIED REPORTS.—Each report submitted under paragraph (1)—

(A) shall be, to the greatest extent practicable, in an unclassified and otherwise uncontrolled form; and

(B) may include 1 or more annexes that contain classified or other sensitive information, as appropriate.

(3) BRIEFINGS.—During each year during which a report is not required to be submitted under paragraph (1), the Director shall provide to the congressional committees described in paragraph (1) a briefing summarizing current agency and Federal risk postures.

[(2)**]***(4)* OTHER PLANS AND REPORTS.—Each agency shall address the adequacy and effectiveness of information security policies, procedures, and practices in management plans and reports**[**.**]**, *including the reporting procedures established under section 11315(d) of title 40 and subsection (a)(3)(A)(v) of this section.*

* * * * * * *

(f) SPECIFIC CYBERSECURITY REQUIREMENTS AT AGENCIES.—

(1) IN GENERAL.—Consistent with policies, standards, guidelines, and directives on information security under this subchapter, and except as provided under paragraph (3), the head of each agency shall—

(A) identify sensitive and mission critical data stored by the agency consistent with the inventory required under section 3505(c);

(B) assess access controls to the data described in subparagraph (A), the need for readily accessible storage of the data, and the need of individuals to access the data;

(C) encrypt or otherwise render indecipherable to unauthorized users the data described in subparagraph (A) that is stored on or transiting agency information systems;

(D) implement a single sign-on trusted identity platform for individuals accessing each public website of the agency that requires user authentication, as developed by the Administrator of General Services in collaboration with the Secretary; and

(E) implement identity management consistent with section 504 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7464), including multi-factor authentication, for—

(i) remote access to an information system; and

(ii) each user account with elevated privileges on a information system.

(2) PROHIBITION.—

(A) DEFINITION.—In this paragraph, the term 'Internet of things' has the meaning given the term in section 3559B.

(B) PROHIBITION.—Consistent with policies, standards, guidelines, and directives on information security under this subchapter, and except as provided under paragraph (3), the head of an agency may not procure, obtain, renew a contract to procure or obtain in any amount, notwithstanding section 1905 of title 41 or use an Internet of things device if the Chief Information Officer of the agency determines during a review required under section 11319(b)(1)(C) of title 40 of a contract for an Internet of things device that the use of the device prevents compliance with the standards and guidelines developed under section 4 of the IoT Cybersecurity Improvement Act (15 U.S.C. 278g–3b) with respect to the device.

(3) EXCEPTION.—The requirements under paragraph (1) shall not apply to an information system for which—

(A) the head of the agency, without delegation, has certified to the Director with particularity that—

(i) operational requirements articulated in the certification and related to the information system would make it excessively burdensome to implement the cybersecurity requirement;

(ii) the cybersecurity requirement is not necessary to secure the information system or agency information stored on or transiting it; and

(iii) the agency has taken all necessary steps to secure the information system and agency information stored on or transiting it; and

(B) the head of the agency has submitted the certification described in subparagraph (A) to the appropriate congressional committees and the authorizing committees of the agency.

(4) DURATION OF CERTIFICATION.—

(A) IN GENERAL.—A certification and corresponding exemption of an agency under paragraph (3) shall expire on the date that is 4 years after the date on which the head

of the agency submits the certification under paragraph (3)(A).

(B) RENEWAL.—Upon the expiration of a certification of an agency under paragraph (3), the head of the agency may submit an additional certification in accordance with that paragraph.

(5) RULES OF CONSTRUCTION.—Nothing in this subsection shall be construed—

(A) to alter the authority of the Secretary, the Director, or the Director of the National Institute of Standards and Technology in implementing subchapter II of this title;

(B) to affect the standards or process of the National Institute of Standards and Technology;

(C) to affect the requirement under section 3553(a)(4); or

(D) to discourage continued improvements and advancements in the technology, standards, policies, and guidelines used to promote Federal information security.

(g) EXCEPTION.—

(1) REQUIREMENTS.—The requirements under subsection (f)(1) shall not apply to—

(A) the Department of Defense;

(B) a national security system; or

(C) an element of the intelligence community.

(2) PROHIBITION.—The prohibition under subsection (f)(2) shall not apply to—

(A) Internet of things devices that are or comprise a national security system;

(B) national security systems; or

(C) a procured Internet of things device described in subsection (f)(2)(B) that the Chief Information Officer of an agency determines is—

(i) necessary for research purposes; or

(ii) secured using alternative and effective methods appropriate to the function of the Internet of things device.

SEC. 3555. [ANNUAL INDEPENDENT] INDEPENDENT EVALUATION.

(a) * * *

(1) Each year *during which a report is required to be submitted under section 3553(c)*, 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) * * *

(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems, *including by performing, or reviewing the results of, agency penetration testing and analyzing the vulnerability disclosure program of the agency*;

* * * * * * *

(3) An evaluation under this section may include recommendations for improving the cybersecurity posture of the agency.

(b) * * *

(1) for each agency with an Inspector General appointed under chapter 4 of title 5, 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

* * * * * * *

(e) * * *

(1) Each year *during which a report is required to be submitted under section 3553(c)*, 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.

* * * * * * *

(g) * * *

(1) * * *

(2) The Director's report to Congress under [this subsection shall] *this subsection—*

(A) 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[.] *; and*

(B) identify any entity that performs an independent evaluation under subsection (b).

* * * * * * *

[(j) GUIDANCE.—The Director, in consultation with the Secretary, the Chief Information Officers Council established under section 3603, the Council of the Inspectors General on Integrity and Efficiency, and other interested parties as appropriate, shall ensure the development of guidance for evaluating the effectiveness of an information security program and practices.]

(j) GUIDANCE.—

(1) IN GENERAL.—The Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, the Chief Information Officers Council, the Council of the Inspectors General on Integrity and Efficiency, and other interested parties as appropriate, shall ensure the development of risk-based guidance for evaluating the effectiveness of an information security program and practices.

(2) PRIORITIES.—The risk-based guidance developed under paragraph (1) shall include—

(A) the identification of the most common successful threat patterns;

(B) the identification of security controls that address the threat patterns described in subparagraph (A);

(C) any other security risks unique to Federal systems; and

(D) any other element the Director determines appropriate.

* * * * * * *

SEC. 3556. FEDERAL INFORMATION SECURITY INCIDENT CENTER.

(a) IN GENERAL.—The Secretary shall ensure the operation of a central Federal information security incident center *within the Cybersecurity and Infrastructure Security Agency* to—

(1) * * *

(2) * * *

(3) * * *

(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)⟧ *3554(a)(1)(A)*; and

* * * * * * *

SEC. 3559A. FEDERAL PENETRATION TESTING.

(a) GUIDANCE.—The Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, shall issue guidance to agencies that—

(1) requires agencies to perform penetration testing on information systems, as appropriate, including on high value assets;

(2) provides policies governing the development of—

(A) rules of engagement for using penetration testing; and

(B) procedures to use the results of penetration testing to improve the cybersecurity and risk management of the agency;

(3) ensures that operational support or a shared service is available; and

(4) in no manner restricts the authority of the Secretary of Homeland Security or the Director of the Cybersecurity and Infrastructure Agency to conduct threat hunting pursuant to section 3553, or penetration testing under this chapter.

(b) EXCEPTION FOR NATIONAL SECURITY SYSTEMS.—The guidance issued under subsection (a) shall not apply to national security systems.

(c) DELEGATION OF AUTHORITY FOR CERTAIN SYSTEMS.—The authorities of the Director described in subsection (a) shall be delegated to—

(1) the Secretary of Defense in the case of a system described in section 3553(e)(2); and

(2) the Director of National Intelligence in the case of a system described in section 3553(e)(3).

SEC. 3559B. FEDERAL VULNERABILITY DISCLOSURE POLICIES.

(a) PURPOSE; SENSE OF CONGRESS.—

(1) PURPOSE.—The purpose of Federal vulnerability disclosure policies is to create a mechanism to enable the public to inform agencies of vulnerabilities in Federal information systems.

(2) SENSE OF CONGRESS.—It is the sense of Congress that, in implementing the requirements of this section, the Federal Government should take appropriate steps to reduce real and perceived burdens in communications between agencies and security researchers.

(b) DEFINITIONS.—In this section:

(1) CONTRACTOR.—The term 'contractor' has the meaning given the term in section 3591.

(2) INTERNET OF THINGS.—The term 'internet of things' has the meaning given the term in Special Publication 800—213 of the National Institute of Standards and Technology, entitled 'IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements', or any successor document.

(3) SECURITY VULNERABILITY.—The term 'security vulnerability' has the meaning given the term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

(4) SUBMITTER.—The term 'submitter' means an individual that submits a vulnerability disclosure report pursuant to the vulnerability disclosure process of an agency.

(5) VULNERABILITY DISCLOSURE REPORT.—The term 'vulnerability disclosure report' means a disclosure of a security vulnerability made to an agency by a submitter.

(c) GUIDANCE.—The Director shall issue guidance to agencies that includes—

(1) use of the information system security vulnerabilities disclosure process guidelines established under section 4(a)(1) of the IoT Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3b(a)(1));

(2) direction to not recommend or pursue legal action against a submitter or an individual that conducts a security research activity that—

(A) represents a good faith effort to identify and report security vulnerabilities in information systems; or

(B) otherwise represents a good faith effort to follow the vulnerability disclosure policy of the agency developed under subsection (f)(2);

(3) direction on sharing relevant information in a consistent, automated, and machine readable manner with the Director of the Cybersecurity and Infrastructure Security Agency;

(4) the minimum scope of agency systems required to be covered by the vulnerability disclosure policy of an agency required under subsection (f)(2), including exemptions under subsection (g);

(5) requirements for providing information to the submitter of a vulnerability disclosure report on the resolution of the vulnerability disclosure report;

(6) a stipulation that the mere identification by a submitter of a security vulnerability, without a significant compromise of confidentiality, integrity, or availability, does not constitute a major incident; and

(7) the applicability of the guidance to Internet of things devices owned or controlled by an agency.

(d) CONSULTATION.—In developing the guidance required under subsection (c)(3), the Director shall consult with the Director of the Cybersecurity and Infrastructure Security Agency.

(e) RESPONSIBILITIES OF CISA.—The Director of the Cybersecurity and Infrastructure Security Agency shall—

(1) provide support to agencies with respect to the implementation of the requirements of this section;

(2) develop tools, processes, and other mechanisms determined appropriate to offer agencies capabilities to implement the requirements of this section;

(3) upon a request by an agency, assist the agency in the disclosure to vendors of newly identified security vulnerabilities in vendor products and services; and

(4) as appropriate, implement the requirements of this section, in accordance with the authority under section 3553(b)(8), as a shared service available to agencies.

(f) RESPONSIBILITIES OF AGENCIES.—

(1) PUBLIC INFORMATION.—The head of each agency shall make publicly available, with respect to each internet domain under the control of the agency that is not a national security system and to the extent consistent with the security of information systems but with the presumption of disclosure—

(A) an appropriate security contact; and

(B) the component of the agency that is responsible for the internet accessible services offered at the domain.

(2) VULNERABILITY DISCLOSURE POLICY.—The head of each agency shall develop and make publicly available a vulnerability disclosure policy for the agency, which shall—

(A) describe—

(i) the scope of the systems of the agency included in the vulnerability disclosure policy, including for Internet of things devices owned or controlled by the agency;

(ii) the type of information system testing that is authorized by the agency;

(iii) the type of information system testing that is not authorized by the agency;

(iv) the disclosure policy for a contractor; and

(v) the disclosure policy of the agency for sensitive information;

(B) with respect to a vulnerability disclosure report to an agency, describe—

(i) how the submitter should submit the vulnerability disclosure report; and

(ii) if the report is not anonymous, when the reporter should anticipate an acknowledgment of receipt of the report by the agency;

(C) include any other relevant information; and

(D) be mature in scope and cover every internet accessible information system used or operated by that agency or on behalf of that agency.

(3) IDENTIFIED SECURITY VULNERABILITIES.—The head of each agency shall—

(A) consider security vulnerabilities reported in accordance with paragraph (2);

(B) commensurate with the risk posed by the security vulnerability, address such security vulnerability using the security vulnerability management process of the agency; and

(C) in accordance with subsection (c)(5), provide information to the submitter of a vulnerability disclosure report.

(g) EXEMPTIONS.—

(1) IN GENERAL.—The Director and the head of each agency shall carry out this section in a manner consistent with the protection of national security information.

(2) LIMITATION.—The Director and the head of each agency may not publish under subsection (f)(1) or include in a vulner-

ability disclosure policy under subsection (f)(2) host names, services, information systems, or other information that the Director or the head of an agency, in coordination with the Director and other appropriate heads of agencies, determines would—

(A) disrupt a law enforcement investigation;

(B) endanger national security or intelligence activities; or

(C) impede national defense activities or military operations.

(3) NATIONAL SECURITY SYSTEMS.—This section shall not apply to national security systems.

(h) DELEGATION OF AUTHORITY FOR CERTAIN SYSTEMS.—The authorities of the Director and the Director of the Cybersecurity and Infrastructure Security Agency described in this section shall be delegated—

(1) to the Secretary of Defense in the case of systems described in section 3553(e)(2); and

(2) to the Director of National Intelligence in the case of systems described in section 3553(e)(3).

(i) REVISION OF FEDERAL ACQUISITION REGULATION.—The Federal Acquisition Regulation shall be revised as necessary to implement the provisions under this section.

* * * * * * *

Subchapter IV—Federal System Incident Response

* * * * * * *

SEC. 3591. DEFINITIONS.

(a) IN GENERAL.—Except as provided in subsection (b), the definitions under sections 3502 and 3552 shall apply to this subchapter.

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

(1) APPROPRIATE REPORTING ENTITIES.—The term 'appropriate reporting entities' means—

(A) the majority and minority leaders of the Senate;

(B) the Speaker and minority leader of the House of Representatives;

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

(D) the Committee on Commerce, Science, and Transportation of the Senate;

(E) the Committee on Oversight and Accountability of the House of Representatives;

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

(G) the Committee on Science, Space, and Technology of the House of Representatives;

(H) the appropriate authorization and appropriations committees of Congress;

(I) the Director;

(J) the Director of the Cybersecurity and Infrastructure Security Agency;

(K) the National Cyber Director;

(L) the Comptroller General of the United States; and

(M) the inspector general of any impacted agency.

(2) AWARDEE.—The term 'awardee', with respect to an agency—

(A) means—

(i) the recipient of a grant from an agency;

(ii) a party to a cooperative agreement with an agency; and

(iii) a party to an other transaction agreement with an agency; and

(B) includes a subawardee of an entity described in subparagraph (A).

(3) BREACH.—The term 'breach'—

(A) means the compromise, unauthorized disclosure, unauthorized acquisition, or loss of control of personally identifiable information or any similar occurrence; and

(B) includes any additional meaning given the term in policies, principles, standards, or guidelines issued by the Director.

(4) CONTRACTOR.—The term 'contractor' means a prime contractor of an agency or a subcontractor of a prime contractor of an agency that creates, collects, stores, processes, maintains, or transmits Federal information on behalf of an agency.

(5) FEDERAL INFORMATION.—The term 'Federal information' means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government in any medium or form.

(6) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' means an information system owned, managed, or operated by an agency, or on behalf of an agency by a contractor, an awardee, or another organization.

(7) INTELLIGENCE COMMUNITY.—The term 'intelligence community' has the meaning given the term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(8) NATIONWIDE CONSUMER REPORTING AGENCY.—The term 'nationwide consumer reporting agency' means a consumer reporting agency described in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

(9) VULNERABILITY DISCLOSURE.—The term 'vulnerability disclosure' means a vulnerability identified under section 3559B.

3592. NOTIFICATION OF BREACH.

(a) DEFINITION.—In this section, the term 'covered breach' means a breach—

(1) involving not less than 50,000 potentially affected individuals; or

(2) the result of which the head of an agency determines that notifying potentially affected individuals is necessary pursuant to subsection (b)(1), regardless of whether—

(A) the number of potentially affected individuals is less than 50,000; or

(B) the notification is delayed under subsection (d).

(b) NOTIFICATION.—As expeditiously as practicable and without unreasonable delay, and in any case not later than 45 days after an agency has a reasonable basis to conclude that a breach has occurred, the head of the agency, in consultation with the Chief Information Officer and Chief Privacy Officer of the agency, shall—

(1) determine whether notice to any individual potentially affected by the breach is appropriate, including by conducting an assessment of the risk of harm to the individual that considers—

(A) the nature and sensitivity of the personally identifiable information affected by the breach;

(B) the likelihood of access to and use of the personally identifiable information affected by the breach;

(C) the type of breach; and

(D) any other factors determined by the Director; and

(2) if the head of the agency determines notification is necessary pursuant to paragraph (1), provide written notification in accordance with subsection (c) to each individual potentially affected by the breach—

(A) to the last known mailing address of the individual; or

(B) through an appropriate alternative method of notification.

(c) CONTENTS OF NOTIFICATION.—Each notification of a breach provided to an individual under subsection (b)(2) shall include, to the maximum extent practicable—

(1) a brief description of the breach;

(2) if possible, a description of the types of personally identifiable information affected by the breach;

(3) contact information of the agency that may be used to ask questions of the agency, which—

(A) shall include an e-mail address or another digital contact mechanism; and

(B) may include a telephone number, mailing address, or a website;

(4) information on any remedy being offered by the agency;

(5) any applicable educational materials relating to what individuals can do in response to a breach that potentially affects their personally identifiable information, including relevant contact information for the appropriate Federal law enforcement agencies and each nationwide consumer reporting agency; and

(6) any other appropriate information, as determined by the head of the agency or established in guidance by the Director.

(d) DELAY OF NOTIFICATION.—

(1) IN GENERAL.—The head of an agency, in coordination with the Director and the National Cyber Director, and as appropriate, the Attorney General, the Director of National Intelligence, or the Secretary of Homeland Security, may delay a notification required under subsection (b) or (e) if the notification would—

(A) impede a criminal investigation or a national security activity;

(B) cause an adverse result (as described in section 2705(a)(2) of title 18);

(C) reveal sensitive sources and methods;

(D) cause damage to national security; or

(E) hamper security remediation actions.

(2) RENEWAL.—A delay under paragraph (1) shall be for a period of 60 days and may be renewed.

(3) NATIONAL SECURITY SYSTEMS.—The head of an agency delaying notification under this subsection with respect to a breach exclusively of a national security system shall coordinate such delay with the Secretary of Defense.

(e) UPDATE NOTIFICATION.—If an agency determines there is a significant change in the reasonable basis to conclude that a breach occurred, a significant change to the determination made under subsection (b)(1), or that it is necessary to update the details of the information provided to potentially affected individuals as described in subsection (c), the agency shall as expeditiously as practicable and without unreasonable delay, and in any case not later than 30 days after such a determination, notify each individual who received a notification pursuant to subsection (b) of those changes.

(f) DELAY OF NOTIFICATION REPORT.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Federal Information Security Modernization Act of 2023, and annually thereafter, the head of an agency, in coordination with any official who delays a notification under subsection (d), shall submit to the appropriate reporting entities a report on each delay that occurred during the previous 2 years.

(2) COMPONENT OF OTHER REPORT.—The head of an agency may submit the report required under paragraph (1) as a component of the report submitted under section 3554(c).

(g) CONGRESSIONAL REPORTING REQUIREMENTS.—

(1) REVIEW AND UPDATE.—On a periodic basis, the Director of the Office of Management and Budget shall review, and update as appropriate, breach notification policies and guidelines for agencies.

(2) REQUIRED NOTICE FROM AGENCIES.—Subject to paragraph (4), the Director of the Office of Management and Budget shall require the head of an agency affected by a covered breach to expeditiously and not later than 30 days after the date on which the agency discovers the covered breach give notice of the breach, which may be provided electronically, to—

(A) each congressional committee described in section 3554(c)(1); and

(B) the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives.

(3) CONTENTS OF NOTICE.—Notice of a covered breach provided by the head of an agency pursuant to paragraph (2) shall include, to the extent practicable—

(A) information about the covered breach, including a summary of any information about how the covered breach occurred known by the agency as of the date of the notice;

(B) an estimate of the number of individuals affected by covered the breach based on information known by the agency as of the date of the notice, including an assessment of the risk of harm to affected individuals;

(C) a description of any circumstances necessitating a delay in providing notice to individuals affected by the covered breach in accordance with subsection (d); and

(D) an estimate of when the agency will provide notice to individuals affected by the covered breach, if applicable.

(4) EXCEPTION.—Any agency that is required to provide notice to Congress pursuant to paragraph (2) due to a covered breach exclusively on a national security system shall only provide such notice to—

(A) the majority and minority leaders of the Senate;

(B) the Speaker and minority leader of the House of Representatives;

(C) the appropriations committees of Congress;

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

(E) the Select Committee on Intelligence of the Senate;

(F) the Committee on Oversight and Accountability of the House of Representatives; and

(G) the Permanent Select Committee on Intelligence of the House of Representatives.

(5) RULE OF CONSTRUCTION.—Nothing in paragraphs (1) through (3) shall be construed to alter any authority of an agency.

(h) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to—

(1) limit—

(A) the authority of the Director to issue guidance relating to notifications of, or the head of an agency to notify individuals potentially affected by, breaches that are not determined to be covered breaches or major incidents;

(B) the authority of the Director to issue guidance relating to notifications and reporting of breaches, covered breaches, or major incidents;

(C) the authority of the head of an agency to provide more information than required under subsection (b) when notifying individuals potentially affected by a breach;

(D) the timing of incident reporting or the types of information included in incident reports provided, pursuant to this subchapter, to—

(i) the Director;

(ii) the National Cyber Director;

(iii) the Director of the Cybersecurity and Infrastructure Security Agency; or

(iv) any other agency;

(E) the authority of the head of an agency to provide information to Congress about agency breaches, including—

(i) breaches that are not covered breaches; and

(ii) additional information beyond the information described in subsection (g)(3); or

(F) any Congressional reporting requirements of agencies under any other law; or

(2) limit or supersede any existing privacy protections in existing law.

3593. CONGRESSIONAL AND EXECUTIVE BRANCH REPORTS ON MAJOR INCIDENTS.

(a) APPROPRIATE CONGRESSIONAL ENTITIES.—In this section, the term 'appropriate congressional entities' means—

(1) the majority and minority leaders of the Senate;

(2) the Speaker and minority leader of the House of Representatives;

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

(4) the Committee on Commerce, Science, and Transportation of the Senate;

(5) the Committee on Oversight and Accountability of the House of Representatives;

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

(7) the Committee on Science, Space, and Technology of the House of Representatives; and

(8) the appropriate authorization and appropriations committees of Congress

(b) INITIAL NOTIFICATION.—

(1) IN GENERAL.—Not later than 72 hours after an agency has a reasonable basis to conclude that a major incident occurred, the head of the agency impacted by the major incident shall submit to the appropriate reporting entities a written notification, which may be submitted electronically and include 1 or more annexes that contain classified or other sensitive information, as appropriate.

(2) CONTENTS.—A notification required under paragraph (1) with respect to a major incident shall include the following, based on information available to agency officials as of the date on which the agency submits the notification:

(A) A summary of the information available about the major incident, including how the major incident occurred and the threat causing the major incident.

(B) If applicable, information relating to any breach associated with the major incident, regardless of whether—

(i) the breach was the reason the incident was determined to be a major incident; and

(ii) head of the agency determined it was appropriate to provide notification to potentially impacted individuals pursuant to section 3592(b)(1).

(C) A preliminary assessment of the impacts to—

(i) the agency;

(ii) the Federal Government;

(iii) the national security, foreign relations, homeland security, and economic security of the United States; and

(iv) the civil liberties, public confidence, privacy, and public health and safety of the people of the United States.

(D) If applicable, whether any ransom has been demanded or paid, or is expected to be paid, by any entity operating a Federal information system or with access to Federal information or a Federal information system, including, as available, the name of the entity demanding ransom, the date of the demand, and the amount and type of currency demanded, unless disclosure of such information will disrupt an active Federal law enforcement or national security operation.

(c) SUPPLEMENTAL UPDATE.—Within a reasonable amount of time, but not later than 30 days after the date on which the head of an agency submits a written notification under subsection (a), the

head of the agency shall provide to the appropriate congressional entities an unclassified and written update, which may include 1 or more annexes that contain classified or other sensitive information, as appropriate, on the major incident, based on information available to agency officials as of the date on which the agency provides the update, on—

(1) system vulnerabilities relating to the major incident, where applicable, means by which the major incident occurred, the threat causing the major incident, where applicable, and impacts of the major incident to—

(A) the agency;

(B) other Federal agencies, Congress, or the judicial branch;

(C) the national security, foreign relations, homeland security, or economic security of the United States; or

(D) the civil liberties, public confidence, privacy, or public health and safety of the people of the United States;

(2) the status of compliance of the affected Federal information system with applicable security requirements at the time of the major incident;

(3) if the major incident involved a breach, a description of the affected information, an estimate of the number of individuals potentially impacted, and any assessment to the risk of harm to such individuals;

(4) an update to the assessment of the risk to agency operations, or to impacts on other agency or non-Federal entity operations, affected by the major incident; and

(5) the detection, response, and remediation actions of the agency, including any support provided by the Cybersecurity and Infrastructure Security Agency under section 3594(d), if applicable.

(d) ADDITIONAL UPDATE.—If the head of an agency, the Director, or the National Cyber Director determines that there is any significant change in the understanding of the scope, scale, or consequence of a major incident for which the head of the agency submitted a written notification and update under subsections (b) and (c), the head of the agency shall submit to the appropriate congressional entities a written update that includes information relating to the change in understanding.

(e) BIENNIAL REPORT.—Each agency shall submit as part of the biennial report required under section 3554(c)(1) a description of each major incident that occurred during the 2-year period preceding the date on which the biennial report is submitted.

(f) REPORT DELIVERY.—

(1) IN GENERAL.—Any written notification or update required to be submitted under this section—

(A) shall be submitted in an electronic format; and

(B) may be submitted in a paper format.

(2) CLASSIFICATION STATUS.—Any written notification or update required to be submitted under this section—

(A) shall be—

(i) unclassified; and

(ii) submitted through unclassified electronic means pursuant to paragraph (1)(A); and

(B) may include classified annexes, as appropriate.

(g) REPORT CONSISTENCY.—To achieve consistent and coherent agency reporting to Congress, the National Cyber Director, in coordination with the Director, shall—

(1) provide recommendations to agencies on formatting and the contents of information to be included in the reports required under this section, including recommendations for consistent formats for presenting any associated metrics; and

(2) maintain a comprehensive record of each major incident notification, update, and briefing provided under this section, which shall—

(A) include, at a minimum—

(i) the full contents of the written notification or update;

(ii) the identity of the reporting agency; and

(iii) the date of submission; and

(iv) a list of the recipient congressional entities; and

(B) be made available upon request to the majority and minority leaders of the Senate, the Speaker and minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Oversight and Accountability of the House of Representatives.

(h) NATIONAL SECURITY SYSTEMS CONGRESSIONAL REPORTING EXEMPTION.—With respect to a major incident that occurs exclusively on a national security system, the head of the affected agency shall submit the notifications and reports required to be submitted to Congress under this section only to—

(1) the majority and minority leaders of the Senate;

(2) the Speaker and minority leader of the House of Representatives;

(3) the appropriations committees of Congress;

(4) the appropriate authorization committees of Congress;

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

(6) the Select Committee on Intelligence of the Senate;

(7) the Committee on Oversight and Accountability of the House of Representatives; and

(8) the Permanent Select Committee on Intelligence of the House of Representatives.

(i) MAJOR INCIDENTS INCLUDING BREACHES.—If a major incident constitutes a covered breach, as defined in section 3592(a), information on the covered breach required to be submitted to Congress pursuant to section 3592(g) may—

(1) be included in the notifications required under subsection (b) or (c); or

(2) be reported to Congress under the process established under section 3592(g).

(j) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to—

(1) limit—

(A) the ability of an agency to provide additional reports or briefings to Congress;

(B) Congress from requesting additional information from agencies through reports, briefings, or other means;

(C) any congressional reporting requirements of agencies under any other law; or

(2) limit or supersede any privacy protections under any other law.

3594. GOVERNMENT INFORMATION SHARING AND INCIDENT RESPONSE.

(a) IN GENERAL.—

(1) INCIDENT SHARING.—Subject to paragraph (4) and subsection (b), and in accordance with the applicable requirements pursuant to section 3553(b)(2)(A) for reporting to the Federal information security incident center established under section 3556, the head of each agency shall provide to the Cybersecurity and Infrastructure Security Agency information relating to any incident affecting the agency, whether the information is obtained by the Federal Government directly or indirectly.

(2) CONTENTS.—A provision of information relating to an incident made by the head of an agency under paragraph (1) shall include, at a minimum—

(A) a full description of the incident, including—

(i) all indicators of compromise and tactics, techniques, and procedures;

(ii) an indicator of how the intruder gained initial access, accessed agency data or systems, and undertook additional actions on the network of the agency; and

(iii) information that would support enabling defensive measures; and

(iv) other information that may assist in identifying other victims;

(B) information to help prevent similar incidents, such as information about relevant safeguards in place when the incident occurred and the effectiveness of those safeguards; and

(C) information to aid in incident response, such as—

(i) a description of the affected systems or networks;

(ii) the estimated dates of when the incident occurred; and

(iii) information that could reasonably help identify any malicious actor that may have conducted or caused the incident, subject to appropriate privacy protections.

(3) INFORMATION SHARING.—The Director of the Cybersecurity and Infrastructure Security Agency shall—

(A) make incident information provided under paragraph (1) available to the Director and the National Cyber Director;

(B) to the greatest extent practicable, share information relating to an incident with—

(i) the head of any agency that may be—

(I) impacted by the incident;

(II) particularly susceptible to the incident; or

(III) similarly targeted by the incident; and

(ii) appropriate Federal law enforcement agencies to facilitate any necessary threat response activities, as requested;

(C) coordinate any necessary information sharing efforts relating to a major incident with the private sector; and

(D) notify the National Cyber Director of any efforts described in subparagraph (C).

(4) NATIONAL SECURITY SYSTEMS EXEMPTION.—

(A) IN GENERAL.—Notwithstanding paragraphs (1) and (3), each agency operating or exercising control of a national security system shall share information about an incident that occurs exclusively on a national security system with the Secretary of Defense, the Director, the National Cyber Director, and the Director of the Cybersecurity and Infrastructure Security Agency to the extent consistent with standards and guidelines for national security systems issued in accordance with law and as directed by the President.

(B) PROTECTIONS.—Any information sharing and handling of information under this paragraph shall be appropriately protected consistent with procedures authorized for the protection of sensitive sources and methods or 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) AUTOMATION.—In providing information and selecting a method to provide information under subsection (a), the head of each agency shall implement subsection (a)(1) in a manner that provides such information to the Cybersecurity and Infrastructure Security Agency in an automated and machine-readable format, to the greatest extent practicable.

(c) INCIDENT RESPONSE.—Each agency that has a reasonable basis to suspect or conclude that a major incident occurred involving Federal information in electronic medium or form that does not exclusively involve a national security system shall coordinate with—

(1) the Cybersecurity and Infrastructure Security Agency to facilitate asset response activities and provide recommendations for mitigating future incidents; and

(2) consistent with relevant policies, appropriate Federal law enforcement agencies to facilitate threat response activities.

3595. RESPONSIBILITIES OF CONTRACTORS AND AWARDEES.

(a) REPORTING.—

(1) IN GENERAL.—Any contractor or awardee of an agency shall report to the agency if the contractor or awardee has a reasonable basis to conclude that—

(A) an incident or breach has occurred with respect to Federal information the contractor or awardee collected, used, or maintained on behalf of an agency;

(B) an incident or breach has occurred with respect to a Federal information system used, operated, managed, or maintained on behalf of an agency by the contractor or awardee;

(C) a component of any Federal information system operated, managed, or maintained by a contractor or awardee contains a security vulnerability, including a supply chain compromise or an identified software or hardware vulnerability, for which there is reliable evidence of attempted or successful exploitation of the vulnerability by an actor with-

out authorization of the Federal information system owner; or

(D) the contractor or awardee has received personally identifiable information, personal health information, or other clearly sensitive information that is beyond the scope of the contract or agreement with the agency from the agency that the contractor or awardee is not authorized to receive.

(2) THIRD-PARTY REPORTS OF VULNERABILITIES.—Subject to the guidance issued by the Director pursuant to paragraph (4), any contractor or awardee of an agency shall report to the agency and the Cybersecurity and Infrastructure Security Agency if the contractor or awardee has a reasonable basis to suspect or conclude that a component of any Federal information system operated, managed, or maintained on behalf of an agency by the contractor or awardee on behalf of the agency contains a security vulnerability, including a supply chain compromise or an identified software or hardware vulnerability, that has been reported to the contractor or awardee by a third party, including through a vulnerability disclosure program.

(3) PROCEDURES.—

(A) SHARING WITH CISA.—As soon as practicable following a report of an incident to an agency by a contractor or awardee under paragraph (1), the head of the agency shall provide, pursuant to section 3594, information about the incident to the Director of the Cybersecurity and Infrastructure Security Agency.

(B) TIME FOR REPORTING.—Unless a different time for reporting is specified in a contract, grant, cooperative agreement, or other transaction agreement, a contractor or awardee shall—

(i) make a report required under paragraph (1) not later than 1 day after the date on which the contractor or awardee has reasonable basis to suspect or conclude that the criteria under paragraph (1) have been met; and

(ii) make a report required under paragraph (2) within a reasonable time, but not later than 90 days after the date on which the contractor or awardee has reasonable basis to suspect or conclude that the criteria under paragraph (2) have been met.

(C) PROCEDURES.—Following a report of a breach or incident to an agency by a contractor or awardee under paragraph (1), the head of the agency, in consultation with the contractor or awardee, shall carry out the applicable requirements under sections 3592, 3593, and 3594 with respect to the breach or incident.

(D) RULE OF CONSTRUCTION.—Nothing in subparagraph (B) shall be construed to allow the negation of the requirements to report vulnerabilities under paragraph (1) or (2) through a contract, grant, cooperative agreement, or other transaction agreement.

(4) GUIDANCE.—The Director shall issue guidance to agencies relating to the scope of vulnerabilities to be reported under paragraph (2), such as the minimum severity of a vulnerability

required to be reported or whether vulnerabilities that are already publicly disclosed must be reported.

(b) REGULATIONS; MODIFICATIONS.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Federal Information Security Modernization Act of 2023—

(A) the Federal Acquisition Regulatory Council shall promulgate regulations, as appropriate, relating to the responsibilities of contractors and recipients of other transaction agreements and cooperative agreements to comply with this section; and

(B) the Office of Federal Financial Management shall promulgate regulations under title 2, Code Federal Regulations, as appropriate, relating to the responsibilities of grantees to comply with this section.

(2) IMPLEMENTATION.—Not later than 1 year after the date on which the Federal Acquisition Regulatory Council and the Office of Federal Financial Management promulgates regulations under paragraph (1), the head of each agency shall implement policies and procedures, as appropriate, necessary to implement those regulations.

(3) CONGRESSIONAL NOTIFICATION.—

(A) IN GENERAL.—The head of each agency head shall notify the Director upon implementation of policies and procedures necessary to implement the regulations promulgated under paragraph (1).

(B) OMB NOTIFICATION.—Not later than 30 days after the date described in paragraph (2), the Director shall notify the Committee on Homeland Security and Governmental Affairs of the Senate and the Committees on Oversight and Accountability and Homeland Security of the House of Representatives on the status of the implementation by each agency of the regulations promulgated under paragraph (1).

(c) NATIONAL SECURITY SYSTEMS EXEMPTION.—Notwithstanding any other provision of this section, a contractor or awardee of an agency that would be required to report an incident or vulnerability pursuant to this section that occurs exclusively on a national security system shall—

(1) report the incident or vulnerability to the head of the agency and the Secretary of Defense; and

(2) comply with applicable laws and policies relating to national security systems.

3596. TRAINING.

(a) COVERED INDIVIDUAL DEFINED.—In this section, the term 'covered individual' means an individual who obtains access to a Federal information system because of the status of the individual as—

(1) an employee, contractor, awardee, volunteer, or intern of an agency; or

(2) an employee of a contractor or awardee of an agency.

(b) BEST PRACTICES AND CONSISTENCY.—The Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director, the National Cyber Director, and the Director of the National Institute of Standards and Technology, shall develop best

practices to support consistency across agencies in cybersecurity incident response training, including—

(1) information to be collected and shared with the Cybersecurity and Infrastructure Security Agency pursuant to section 3594(a) and processes for sharing such information; and

(2) appropriate training and qualifications for cyber incident responders.

(c) AGENCY TRAINING.—The head of each agency shall develop training for covered individuals on how to identify and respond to an incident, including—

(1) the internal process of the agency for reporting an incident; and

(2) the obligation of a covered individual to report to the agency any suspected or confirmed incident involving Federal information in any medium or form, including paper, oral, and electronic.

(d) INCLUSION IN ANNUAL TRAINING.—The training developed under subsection (c) may be included as part of an annual privacy, security awareness, or other appropriate training of an agency.

3597. ANALYSIS AND REPORT ON FEDERAL INCIDENTS.

(a) ANALYSIS OF FEDERAL INCIDENTS.—

(1) QUANTITATIVE AND QUALITATIVE ANALYSES.—The Director of the Cybersecurity and Infrastructure Security Agency shall perform and, in coordination with the Director and the National Cyber Director, develop, continuous monitoring and quantitative and qualitative analyses of incidents at agencies, including major incidents, including—

(A) the causes of incidents, including—

(i) attacker tactics, techniques, and procedures; and

(ii) system vulnerabilities, including zero days, unpatched systems, and information system misconfigurations;

(B) the scope and scale of incidents at agencies;

(C) common root causes of incidents across multiple agencies;

(D) agency incident response, recovery, and remediation actions and the effectiveness of those actions, as applicable;

(E) lessons learned and recommendations in responding to, recovering from, remediating, and mitigating future incidents; and

(F) trends across multiple agencies to address intrusion detection and incident response capabilities using the metrics established under section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c)).

(2) AUTOMATED ANALYSIS.—The analyses developed under paragraph (1) shall, to the greatest extent practicable, use machine readable data, automation, and machine learning processes.

(3) SHARING OF DATA AND ANALYSIS.—

(A) IN GENERAL.—The Director of the Cybersecurity and Infrastructure Security Agency shall share on an ongoing basis the analyses and underlying data required under this subsection with agencies, the Director, and the National Cyber Director to—

(i) improve the understanding of cybersecurity risk of agencies; and

(ii) support the cybersecurity improvement efforts of agencies.

(B) FORMAT.—In carrying out subparagraph (A), the Director of the Cybersecurity and Infrastructure Security Agency shall share the analyses—

(i) in human-readable written products; and

(ii) to the greatest extent practicable, in machine-readable formats in order to enable automated intake and use by agencies.

(C) EXEMPTION.—This subsection shall not apply to incidents that occur exclusively on national security systems.

(b) ANNUAL REPORT ON FEDERAL INCIDENTS.—Not later than 2 years after the date of enactment of this section, and not less frequently than annually thereafter, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director, the National Cyber Director and the heads of other agencies, as appropriate, shall submit to the appropriate reporting entities a report that includes—

(1) a summary of causes of incidents from across the Federal Government that categorizes those incidents as incidents or major incidents;

(2) the quantitative and qualitative analyses of incidents developed under subsection (a)(1) on an agency-by-agency basis and comprehensively across the Federal Government, including—

(A) a specific analysis of breaches; and

(B) an analysis of the Federal Government's performance against the metrics established under section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c)); and

(3) an annex for each agency that includes—

(A) a description of each major incident;

(B) the total number of incidents of the agency; and

(C) an analysis of the agency's performance against the metrics established under section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c)).

(c) PUBLICATION.—

(1) IN GENERAL.—The Director of the Cybersecurity and Infrastructure Security Agency shall make a version of each report submitted under subsection (b) publicly available on the website of the Cybersecurity and Infrastructure Security Agency during the year during which the report is submitted.

(2) EXEMPTION.—The publication requirement under paragraph (1) shall not apply to a portion of a report that contains content that should be protected in the interest of national security, as determined by the Director, the Director of the Cybersecurity and Infrastructure Security Agency, or the National Cyber Director.

(3) LIMITATION ON EXEMPTION.—The exemption under paragraph (2) shall not apply to any version of a report submitted to the appropriate reporting entities under subsection (b).

(4) REQUIREMENT FOR COMPILING INFORMATION.—

(A) COMPILATION.—Subject to subparagraph (B), in making a report publicly available under paragraph (1), the Di-

rector of the Cybersecurity and Infrastructure Security Agency shall sufficiently compile information so that no specific incident of an agency can be identified.

(B) EXCEPTION.—The Director of the Cybersecurity and Infrastructure Security Agency may include information that enables a specific incident of an agency to be identified in a publicly available report—

(i) with the concurrence of the Director and the National Cyber Director;

(ii) in consultation with the impacted agency; and

(iii) in consultation with the inspector general of the impacted agency.

(d) INFORMATION PROVIDED BY AGENCIES.—

(1) IN GENERAL.—The analysis required under subsection (a) and each report submitted under subsection (b) shall use information provided by agencies under section 3594(a).

(2) NONCOMPLIANCE REPORTS.—During any year during which the head of an agency does not provide data for an incident to the Cybersecurity and Infrastructure Security Agency in accordance with section 3594(a), the head of the agency, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and the Director, shall submit to the appropriate reporting entities a report that includes the information described in subsection (b) with respect to the agency.

(e) NATIONAL SECURITY SYSTEM REPORTS.—

(1) IN GENERAL.—Notwithstanding any other provision of this section, the Secretary of Defense, in consultation with the Director, the National Cyber Director, the Director of National Intelligence, and the Director of Cybersecurity and Infrastructure Security shall annually submit a report that includes the information described in subsection (b) with respect to national security systems, to the extent that the submission is consistent with standards and guidelines for national security systems issued in accordance with law and as directed by the President, to—

(A) the majority and minority leaders of the Senate;

(B) the Speaker and minority leader of the House of Representatives;

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

(D) the Select Committee on Intelligence of the Senate;

(E) the Committee on Armed Services of the Senate;

(F) the Committee on Appropriations of the Senate;

(G) the Committee on Oversight and Accountability of the House of Representatives;

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

(I) the Permanent Select Committee on Intelligence of the House of Representatives;

(J) the Committee on Armed Services of the House of Representatives; and

(K) the Committee on Appropriations of the House of Representatives.

(2) CLASSIFIED FORM.—A report required under paragraph (1) may be submitted in a classified form.

3598. MAJOR INCIDENT DEFINITION.

(a) IN GENERAL.—Not later than 1 year after the later of the date of enactment of the Federal Information Security Modernization Act of 2023 and the most recent publication by the Director of guidance to agencies regarding major incidents as of the date of enactment of the Federal Information Security Modernization Act of 2023, the Director shall develop, in coordination with the National Cyber Director, and promulgate guidance on the definition of the term 'major incident' for the purposes of subchapter II and this subchapter.

(b) REQUIREMENTS.—With respect to the guidance issued under subsection (a), the definition of the term 'major incident' shall—

(1) include, with respect to any information collected or maintained by or on behalf of an agency or a Federal information system—

(A) any incident the head of the agency determines is likely to result in demonstrable harm to—

(i) the national security interests, foreign relations, homeland security, or economic security of the United States; or

(ii) the civil liberties, public confidence, privacy, or public health and safety of the people of the United States;

(B) any incident the head of the agency determines likely to result in an inability or substantial disruption for the agency, a component of the agency, or the Federal Government, to provide 1 or more critical services;

(C) any incident the head of the agency determines substantially disrupts or substantially degrades the operations of a high value asset owned or operated by the agency;

(D) any incident involving the exposure to a foreign entity of sensitive agency information, such as the communications of the head of the agency, the head of a component of the agency, or the direct reports of the head of the agency or the head of a component of the agency; and

(E) any other type of incident determined appropriate by the Director;

(2) stipulate that the National Cyber Director, in consultation with the Director and the Director of the Cybersecurity and Infrastructure Security Agency, may declare a major incident at any agency, and such a declaration shall be considered if it is determined that an incident—

(A) occurs at not less than 2 agencies; and

(B) is enabled by—

(i) a common technical root cause, such as a supply chain compromise, or a common software or hardware vulnerability; or

(ii) the related activities of a common threat actor;

(3) stipulate that, in determining whether an incident constitutes a major incident under the standards described in paragraph (1), the head of the agency shall consult with the National Cyber Director; and

(4) stipulate that the mere report of a vulnerability discovered or disclosed without a loss of confidentiality, integrity, or availability shall not on its own constitute a major incident.

(c) EVALUATION AND UPDATES.—Not later than 60 days after the date on which the Director first promulgates the guidance required under subsection (a), and not less frequently than once during the first 90 days of each evenly numbered Congress thereafter, the Director shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committees on Oversight and Accountability and Homeland Security of the House of Representatives a briefing that includes—

(1) an evaluation of any necessary updates to the guidance;

(2) an evaluation of any necessary updates to the definition of the term 'major incident' included in the guidance; and

(3) an explanation of, and the analysis that led to, the definition described in paragraph (2).

CHAPTER 36—MANAGEMENT AND PROMOTION OF ELECTRONIC GOVERNMENT SERVICES

* * * * * * *

SEC. 3601. DEFINITIONS.

In this chapter, the definitions under section 3502 shall apply, and the term—

[(1) "Administrator" means the Administrator of the Office of Electronic Government established under section 3602;]

[(2)]*(1)* * * *

[(3)]*(2)* * * *

[(4)]*(3)* * * *

[(5)]*(4)* * * *

[(6)]*(5)* * * *

[(7)]*(6)* * * *

[(8)]*(7)* * * *

* * * * * * *

SEC. 3602. [OFFICE OF ELECTRONIC GOVERNMENT] *OFFICE OF THE FEDERAL CHIEF INFORMATION OFFICER.*

(a) There is established in the Office of Management and Budget an Office of Electronic Government *Office of the Federal Chief Information Officer*.

(b) There shall be at the head of the Office [an Administrator] a *Federal Chief Information Officer* who shall be appointed by the President.

(c) [The Administrator] *The Federal Chief Information Officer* shall assist the Director in carrying out—

* * * * * * *

(d) [The Administrator] *The Federal Chief Information Officer* shall assist the Director and the Deputy Director for Management and work with the Administrator of the Office of Information and

Regulatory Affairs in setting strategic direction for implementing electronic Government, under relevant statutes, including—

* * * * * * *

(e) [The Administrator] *The Federal Chief Information Officer* shall work with the Administrator of the Office of Information and Regulatory Affairs and with other offices within the Office of Management and Budget to oversee implementation of electronic Government under this chapter,chapter 35, the E-Government Act of 2002, and other relevant statutes, in a manner consistent with law, relating to—

* * * * * * *

(f) Subject to requirements of this chapter, [the Administrator] *the Federal Chief Information Officer* shall assist the Director by performing electronic Government functions as follows:

* * * * * * *

(16) Administer [the Office of Electronic Government] *the Office of the Federal Chief Information Officer* established under this section.

(17) Assist the Director in preparing the [E-Government] *annual* report established under section 3606.

(g) The Director shall ensure that the Office of Management and Budget, including [the Office of Electronic Government] *the Office of the Federal Chief Information Officer*, the Office of Information and Regulatory Affairs, and other relevant offices, have adequate staff and resources to properly fulfill all functions under the E Government Act of 2002.

* * * * * * *

SEC. 3603. CHIEF INFORMATION OFFICERS COUNCIL.

(a) * * *

(b) * * *

(1) * * *

(2) [The Administrator of the Office of Electronic Government] *The Federal Chief Information Officer*.

* * * * * * *

(c)(1) [The Administrator of the Office of Electronic Government] *The Federal Chief Information Officer* shall lead the activities of the Council on behalf of the Deputy Director for Management.

* * * * * * *

(f) * * *

(1) * * *

(2) * * *

(3) Assist [the Administrator] *the Federal Chief Information Officer* in the identification, development, and coordination of multiagency projects and other innovative initiatives to improve Government performance through the use of information technology.

(4) * * *

(5) Work as appropriate with the National Institute of Standards and Technology and [the Administrator] *the Federal Chief Information Officer* to develop recommendations on information technology standards developed under section 20 of the

National Institute of Standards and Technology Act (15 U.S.C. 278g–3) and promulgated undersection 11331 of title 40, and maximize the use of commercial standards as appropriate, including the following:

* * * * * * *

SEC. 3604. E-GOVERNMENT FUND.

(a)

(1) * * *

(2) The Fund shall be administered by the Administrator of the General Services Administration to support projects approved by the Director, assisted by [the Administrator of the Office of Electronic Government] *the Federal Chief Information Officer*, that enable the Federal Government to expand its ability, through the development and implementation of innovative uses of the Internet or other electronic methods, to conduct activities electronically.

* * * * * * *

(b)(1) [The Administrator] *The Federal Chief Information Officer* shall—

* * * * * * *

(c) In determining which proposals to recommend for funding, [the Administrator] *the Federal Chief Information Officer*—

* * * * * * *

SEC. 3605. PROGRAM TO ENCOURAGE INNOVATIVE SOLUTIONS TO ENHANCE ELECTRONIC GOVERNMENT SERVICES AND PROCESSES.

(a) ESTABLISHMENT OF PROGRAM.—[The Administrator] *The Federal Chief Information Officer* shall establish and promote a Governmentwide program to encourage contractor innovation and excellence in facilitating the development and enhancement of electronic Government services and processes.

(b) ISSUANCE OF ANNOUNCEMENTS SEEKING INNOVATIVE SOLUTIONS.—Under the program, [the Administrator] *the Federal Chief Information Officer*, in consultation with the Council and the Administrator for Federal Procurement Policy, shall issue announcements seeking unique and innovative solutions to facilitate the development and enhancement of electronic Government services and processes.

(c) MULTIAGENCY TECHNICAL ASSISTANCE TEAM.—(1) [The Administrator] *The Federal Chief Information Officer*, in consultation with the Council and the Administrator for Federal Procurement Policy, shall convene a multiagency technical assistance team to assist in screening [proposals submitted to the Administrator] *proposals submitted to the Federal Chief Information Officer* to provide unique and innovative solutions to facilitate the development and enhancement of electronic Government services and processes. The team shall be composed of employees of the agencies represented on the Council who have expertise in scientific and technical disciplines that would facilitate the assessment of the feasibility of the proposals.

(2) * * *

(A) * * *

(B) submit each proposal, and the assessment of the proposal, to [the Administrator] *the Federal Chief Information Officer*.

(3) * * *

(4) After receiving proposals and assessments from the technical assistance team, [the Administrator] *the Federal Chief Information Officer* shall consider recommending appropriate proposals for funding under the E-Government Fund established under section 3604 or, if appropriate, forward the proposal and the assessment of it to the executive agency whose mission most coincides with the subject matter of the proposal.

* * * * * * *

SEC. 3606. [E-GOVERNMENT] *ANNUAL* REPORT.

(a) Not later than March 1 of each year, the Director shall submit an [E-Government] *annual* status report to the Committee on Governmental Affairs of the Senate and the Committee on Government Reform of the House of Representatives.

(b) The report under subsection (a) shall contain—

(1) a summary of the information reported by agencies under section [202(f)] *202(g)* of the E-Government Act of 2002;

* * * * * * *

SEC. 3617. FEDERAL CHIEF INFORMATION SECURITY OFFICER.

(a) ESTABLISHMENT.—There is established a Federal Chief Information Security Officer, who shall serve in—

(1) the Office of the Federal Chief Information Officer of the Office of Management and Budget; and

(2) the Office of the National Cyber Director.

(b) APPOINTMENT.—The Federal Chief Information Security Officer shall be appointed by the President.

(c) OMB DUTIES.—The Federal Chief Information Security Officer shall report to the Federal Chief Information Officer and assist the Federal Chief Information Officer in carrying out—

(1) every function under this chapter;

(2) every function assigned to the Director under title II of the E-Government Act of 2002 (44 U.S.C. 3501 note; Public Law 107–347);

(3) other electronic government initiatives consistent with other statutes; and

(4) other Federal cybersecurity initiatives determined by the Federal Chief Information Officer.

(d) ADDITIONAL DUTIES.—The Federal Chief Information Security Officer shall—

(1) support the Federal Chief Information Officer in overseeing and implementing Federal cybersecurity under the E—Government Act of 2002 (Public Law 107–347; 116 Stat. 2899) and other relevant statutes in a manner consistent with law; and

(2) perform every function assigned to the Director under sections 1321 through 1328 of title 41, United States Code.

(e) COORDINATION WITH ONCD.—The Federal Chief Information Security Officer shall support initiatives determined by the Federal

Chief Information Officer necessary to coordinate with the Office of the National Cyber Director.

* * * * * * *

HOMELAND SECURITY ACT OF 2002

* * * * * * *

TITLE X—INFORMATION SECURITY

* * * * * * *

SEC. 1001. INFORMATION SECURITY.

(a) * * *

(b) * * *

(c) INFORMATION SECURITY RESPONSIBILITIES OF CERTAIN AGENCIES.—

(1) NATIONAL SECURITY RESPONSIBILITIES.—(A) Nothing in this Act (including any amendment made by this Act) shall supersede 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 3552(b)(5)**]** *section 3552(b)* of title 44, United States Code.

* * * * * * *

CONSOLIDATED APPROPRIATIONS ACT, 2016

* * * * * * *

DIVISION N—CYBERSECURITY ACT OF 2015

* * * * * * *

TITLE II—NATIONAL CYBERSECURITY ADVANCEMENT

* * * * * * *

Subtitle B—Federal Cybersecurity Enhancement

SEC. 221. * * *

SEC. 222. DEFINITIONS.

In this subtitle:

(1) * * *

(2) * * *

(3) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" means—

(A) * * *

(B) the Committee on Homeland Security *and the Committee on Oversight and Accountability* of the House of Representatives.

* * * * * * *

SEC. 225. FEDERAL CYBERSECURITY REQUIREMENTS.

(a) * * *

[(b) Cybersecurity Requirements at Agencies.—

[(1) IN GENERAL.—Consistent with policies, standards, guidelines, and directives on information security under subchapter II of chapter 35 of title 44 and the standards and guidelines promulgated under section 11331 of title 40 and except as provided in paragraph (2), not later than 1 year after December 18, 2015, the head of each agency shall—

[(A) identify sensitive and mission critical data stored by the agency consistent with the inventory required under the first subsection (c) (relating to the inventory of major information systems) and the second subsection (c) (relating to the inventory of information systems) of section 3505 of title 44;

[(B) assess access controls to the data described in subparagraph (A), the need for readily accessible storage of the data, and individuals' need to access the data;

[(C) encrypt or otherwise render indecipherable to unauthorized users the data described in subparagraph (A) that is stored on or transiting agency information systems;

[(D) implement a single sign-on trusted identity platform for individuals accessing each public website of the agency that requires user authentication, as developed by the Administrator of General Services in collaboration with the Secretary; and

[(E) implement identity management consistent with section 7464 of title 15, including multi-factor authentication, for—

[(i) remote access to an agency information system; and

[(ii) each user account with elevated privileges on an agency information system.

[(2) EXCEPTION.—The requirements under paragraph (1) shall not apply to an agency information system for which—

[(A) the head of the agency has personally certified to the Director with particularity that—

[(i) operational requirements articulated in the certification and related to the agency information system would make it excessively burdensome to implement the cybersecurity requirement;

[(ii) the cybersecurity requirement is not necessary to secure the agency information system or agency information stored on or transiting it; and

[(iii) the agency has taken all necessary steps to secure the agency information system and agency information stored on or transiting it; and

[(B) the head of the agency or the designee of the head of the agency has submitted the certification described in

subparagraph (A) to the appropriate congressional committees and the agency's authorizing committees.

[(3) CONSTRUCTION.—Nothing in this section shall be construed to alter the authority of the Secretary, the Director, or the Director of the National Institute of Standards and Technology in implementing subchapter II of chapter 35 of title 44. Nothing in this section shall be construed to affect the National Institute of Standards and Technology standards process or the requirement under section 3553(a)(4) of such title or to discourage continued improvements and advancements in the technology, standards, policies, and guidelines used to promote Federal information security.

[(c) EXCEPTION.—The requirements under this section shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.]

SEC. 226. ASSESSMENT; REPORTS.

(a) * * *

(b) * * *

(c) * * *

(1) * * *

(A) * * *

(B) OMB REPORT.—Not later than 18 months after December 18, 2015, and [annually thereafter] *thereafter during the years during which a report is required to be submitted under section 3553(c) of title 44, United States Code*, the Director shall submit to Congress, as part of the report required undersection 3553(c) of title 44, an analysis of agency application of the intrusion detection and prevention capabilities, including—

* * * * * * *

(2) * * *

(A) * * *

(B) not later than 1 year after December 18, 2015, and [annually thereafter] *thereafter during the years during which a report is required to be submitted under section 3553(c) of title 44, United States Code*, submit to Congress, as part of [the report required undersection 3553(c) of title 44, United States Code] *that report*.

* * * * * * *

WILLIAM M. (MAC) THORNBERRY NATIONAL DEFENSE AUTHORIZATION ACT

FOR FISCAL YEAR 2021

* * * * * * *

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

* * * * * * *

TITLE XVII—CYBERSPACE RELATED MATTERS

* * * * * * *

SEC. 1752. NATIONAL CYBER DIRECTOR.

(a) * * *

* * * * * * *

(f) * * *

(g) SENIOR FEDERAL CYBERSECURITY OFFICER.—The Federal Chief Information Security Officer appointed by the President under section 3617 of title 44, United States Code, shall be a senior official within the Office and carry out duties applicable to the protection of information technology (as defined in section 11101 of title 40, United States Code), including initiatives determined by the Director necessary to coordinate with the Office of the Federal Chief Information Officer.

[(g)**]**(*h*) * * *

* * * * * * *

HIGH PERFORMANCE COMPUTING ACT OF 1991

* * * * * * *

TITLE II—AGENCY ACTIVITIES

* * * * * * *

SEC. 207. MISCELLANEOUS PROVISIONS.

(a) * * *

(1) * * *

(2) computer systems the function, operation, or use of which are those delineated in **[**section 3552(b)(6)(A)(i)**]** *section 3552(b)(8)(A)(i)* of title 44, United States Code.

* * * * * * *

INTERNET OF THINGS CYBERSECURITY IMPROVEMENT ACT OF 2020

* * * * * * *

SEC. 3. DEFINITIONS.

* * * * * * *

(5) NATIONAL SECURITY SYSTEM.—The term "national security system" has the meaning given that term in **[**section 3552(b)(6)**]** *3552(b)* of title 44, United States Code.

* * * * * * *

SEC. 5. GUIDELINES ON THE DISCLOSURE PROCESS FOR SECURITY VULNERABILITIES RELATING TO INFORMATION SYSTEMS, INCLUDING INTERNET OF THINGS DEVICES.

(a) * * *

(b) * * *

(c) * * *

[(d) OVERSIGHT.—The Director of OMB shall oversee the implementation of the guidelines published under subsection (a).

[(e) OPERATIONAL AND TECHNICAL ASSISTANCE.—The Secretary, in consultation with the Director of OMB, shall administer the implementation of the guidelines published under subsection (a) and provide operational and technical assistance in implementing such guidelines.]

* * * * * * *

[SEC. 6. IMPLEMENTATION OF COORDINATED DISCLOSURE OF SECURITY VULNERABILITIES RELATING TO AGENCY INFORMATION SYSTEMS, INCLUDING INTERNET OF THINGS DEVICES.

[(a) AGENCY GUIDELINES REQUIRED.—Not later than 2 years after the date of the enactment of this Act, the Director of OMB, in consultation with the Secretary, shall develop and oversee the implementation of policies, principles, standards, or guidelines as may be necessary to address security vulnerabilities of information systems (including Internet of Things devices).

[(b) OPERATIONAL AND TECHNICAL ASSISTANCE.—Consistent with section 3553(b) of title 44, United States Code, the Secretary, in consultation with the Director of OMB, shall provide operational and technical assistance to agencies on reporting, coordinating, publishing, and receiving information about security vulnerabilities of information systems (including Internet of Things devices).

[(c) CONSISTENCY WITH GUIDELINES FROM NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.—The Secretary shall ensure that the assistance provided under subsection (b) is consistent with applicable standards and publications developed by the Director of the Institute.

[(d) REVISION OF FEDERAL ACQUISITION REGULATION.—The Federal Acquisition Regulation shall be revised as necessary to implement the provisions under this section.

[SEC. 7. CONTRACTOR COMPLIANCE WITH COORDINATED DISCLOSURE OF SECURITY VULNERABILITIES RELATING TO AGENCY INTERNET OF THINGS DEVICES.

[(a) PROHIBITION ON PROCUREMENT AND USE.—

[(1) IN GENERAL.—The head of an agency is prohibited from procuring or obtaining, renewing a contract to procure or obtain, or using an Internet of Things device, if the Chief Information Officer of that agency determines during a review required by section 11319(b)(1)(C) of title 40, United States Code, of a contract for such device that the use of such device prevents compliance with the standards and guidelines developed under section 4 or the guidelines published under section 5 with respect to such device.

[(2) SIMPLIFIED ACQUISITION THRESHOLD.—Notwithstanding section 1905 of title 41, United States Code, the requirements under paragraph (1) shall apply to a contract or subcontract in amounts not greater than the simplified acquisition threshold.

[(b) WAIVER.—

[(1) AUTHORITY.—The head of an agency may waive the prohibition under subsection (a)(1) with respect to an Internet of Things device if the Chief Information Officer of that agency determines that—

[(A) the waiver is necessary in the interest of national security;

[(B) procuring, obtaining, or using such device is necessary for research purposes; or

[(C) such device is secured using alternative and effective methods appropriate to the function of such device.

[(2) AGENCY PROCESS.—The Director of OMB shall establish a standardized process for the Chief Information Officer of each agency to follow in determining whether the waiver under paragraph (1) may be granted.

[(c) REPORTS TO CONGRESS.—

[(1) REPORT.—Every 2 years during the 6-year period beginning on the date of the enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate a report—

[(A) on the effectiveness of the process established under subsection (b)(2);

[(B) that contains recommended best practices for the procurement of Internet of Things devices; and

[(C) that lists—

[(i) the number and type of each Internet of Things device for which a waiver under subsection (b)(1) was granted during the 2-year period prior to the submission of the report; and

[(ii) the legal authority under which each such waiver was granted, such as whether the waiver was granted pursuant to subparagraph (A), (B), or (C) of such subsection.

[(2) CLASSIFICATION OF REPORT.—Each report submitted under this subsection shall be submitted in unclassified form, but may include a classified annex that contains the information described under paragraph (1)(C).

[(d) EFFECTIVE DATE.—The prohibition under subsection (a)(1) shall take effect 2 years after the date of the enactment of this Act.]

* * * * * * *

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2013

* * * * * * *

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

* * * * * * *

TITLE IX—DEPARTMENT OF DEFENSE ORGANIZATION AND MANAGEMENT

* * * * * * *

Subtitle D—Cyberspace Related Matters

* * * * * * *

SEC. 933. IMPROVEMENTS IN ASSURANCE OF COMPUTER SOFTWARE PROCURED BY THE DEPARTMENT OF DEFENSE.

* * * * * * *

(e) * * *

(1) * * *

(A) * * *

(B) a national security system, as that term is defined in section [3542(b)(2)] *3552(b)* of title 44, United Sates Code; or

* * * * * * *

IKE SKELTON NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011

* * * * * * *

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

* * * * * * *

TITLE VIII—ACQUISITION POLICY, ACQUISITION MANAGEMENT, AND RELATED MATTERS

* * * * * * *

Subtitle A—Acquisition Policy and Management

* * * * * * *

SEC. 806. REQUIREMENTS FOR INFORMATION RELATING TO SUPPLY CHAIN RISK.

* * * * * * *

(e) * * *

(1) * * *

(2) * * *

(3) * * *

(4) * * *

(5) COVERED SYSTEM.—The term "covered system" means a national security system, as that term is defined in section [3542(b)] 3552(b) of title 44, United States Code.

* * * * * * *

TITLE IX—DEPARTMENT OF DEFENSE ORGANIZATION AND MANAGEMENT

* * * * * * *

Subtitle D—Cyber Warfare, Cyber Security, and Related Matters

* * * * * * *

SEC. 931. CONTINUOUS MONITORING OF DEPARTMENT OF DEFENSE INFORMATION SYSTEMS FOR CYBERSECURITY.

(a) * * *
(b) * * *
(1) * * *
(2) * * *
(3) The term "national security system" has the meaning given that term in section [3542(b)(2)] *3552(b)* of title 44, United States Code.

SEC. 932. STRATEGY ON COMPUTER SOFTWARE ASSURANCE.

(a) * * *
(b) * * *
(1) * * *
(2) A national security system, as that term is defined in section [3542(b)(2)] *3552(b)* of title 44, United States Code.

* * * * * * *

E GOVERNMENT ACT OF 2002

* * * * * * *

TITLE III—INFORMATION SECURITY

SEC. 301. INFORMATION SECURITY.

* * * * * * *

(c) * * *
(1) NATIONAL SECURITY RESPONSIBILITIES.—(A) Nothing in this Act (including any amendment made by this Act) shall supersede 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 [3542(b)(2)] *3552(b)* of title 44, United States Code.

* * * * * * *

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ACT

* * * * * * *

SEC. 20.

(a) * * *

(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 3552(b)(6)] *section 3552(b)* of title 44) United States Code;

* * * * * * *

(d) * * *

(1) * * *

(2) * * *

(3) * * *

(A) * * *

(B) to review and determine prevalent information security challenges and deficiencies identified by agencies or the Institute, including any challenges or deficiencies described in any of the [annual] reports undersection 3553 or 3554 of title 44, United States Code, and in any of the reports and the independent evaluations under section 3555 of that title, that may undermine the effectiveness of agency information security programs and practices; and

* * * * * * *

(f) * * *

(1) * * *

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

(3) * * *

(4) * * *

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

* * * * * * *

FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014

SEC. 1. * * *

SEC. 2. FISMA REFORM.

(a) * * *

[(b) MAJOR INCIDENT.—The Director of the Office of Management and Budget shall—

[(1) develop guidance on what constitutes a major incident for purposes of section 3554(b) of title 44, United States Code, as added by subsection (a); and

[(2) provide to Congress periodic briefings on the status of the developing of the guidance until the date on which the guidance is issued.]

[(c)]*(b)* * * *

[(d) BREACHES.—

[(1) REQUIREMENTS.—The Director of the Office of Management and Budget shall ensure that data breach notification policies and guidelines are updated periodically and require—

[(A) except as provided in paragraph (4), notice by the affected agency to each committee of Congress described in section 3554(c)(1) of title 44, United States Code, as added by subsection (a), the Committee on the Judiciary of the Senate, and the Committee on the Judiciary of the House of Representatives, which shall—

[(i) be provided expeditiously and not later than 30 days after the date on which the agency discovered the unauthorized acquisition or access; and

[(ii) include—

[(I) information about the breach, including a summary of any information that the agency knows on the date on which notification is provided about how the breach occurred;

[(II) an estimate of the number of individuals affected by the breach, based on information that the agency knows on the date on which notification is provided, including an assessment of the risk of harm to affected individuals;

[(III) a description of any circumstances necessitating a delay in providing notice to affected individuals; and

[(IV) an estimate of whether and when the agency will provide notice to affected individuals; and

[(B) notice by the affected agency to affected individuals, pursuant to data breach notification policies and guidelines, which shall be provided as expeditiously as practicable and without unreasonable delay after the agency discovers the unauthorized acquisition or access.

[(2) NATIONAL SECURITY; LAW ENFORCEMENT; REMEDIATION.—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 of Homeland Security may delay the notice to affected individuals under paragraph (1)(B) if the notice would disrupt a law enforcement investigation, endanger national security, or hamper security remediation actions.

[(3) REPORTS.—

[(A) DIRECTOR OF OMB.—During the first 2 years beginning after the date of enactment of this Act, the Director of the Office of Management and Budget shall, on an annual basis—

[(i) assess agency implementation of data breach notification policies and guidelines in aggregate; and

[(ii) include the assessment described in clause (i) in the report required under section 3553(c) of title 44, United States Code.

[(B) SECRETARY OF HOMELAND SECURITY.—During the first 2 years beginning after the date of enactment of this Act, the Secretary of Homeland Security shall include an assessment of the status of agency implementation of data breach notification policies and guidelines in the requirements under section 3553(b)(2)(B) of title 44, United States Code.

[(4) EXCEPTION.—Any 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)) that is required to provide notice under paragraph (1)(A) shall only provide such notice to appropriate committees of Congress.

[(5) RULE OF CONSTRUCTION.—Nothing in paragraph (1) shall be construed to alter any authority of a Federal agency or department.]

[(e)]*(c)* * * *

[(f)]*(d)* * * *

* * * * * * *

NATIONAL SECURITY ACT OF 1947

* * * * * * *

TITLE V—ACCOUNTABILITY FOR INTELLIGENCE ACTIVITIES

* * * * * * *

SEC. 506D.

(a) * * *

* * * * * * *

(k) * * *

(1) The term "enterprise architecture" has the meaning given that term in [section 3601(4)] *section 3601* of title 44, United States Code.

* * * * * * *

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2018

* * * * * * *

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

* * * * * * *

TITLE X—GENERAL PROVISIONS

* * * * * * *

Subtitle G—Modernizing Government Technology

* * * * * * *

SEC. 1078. ESTABLISHMENT OF TECHNOLOGY MODERNIZATION FUND AND BOARD.

[(a) DEFINITION.— In this section, the term 'agency' has the meaning given the term in section 551 of title 5, United States Code.]

(a) DEFINITIONS.—In this section:

(1) AGENCY.—The term 'agency' has the meaning given the term in section 551 of title 5, United States Code.

(2) HIGH VALUE ASSET.—The term 'high value asset' has the meaning given the term in section 3552 of title 44, United States Code.

(b) * * *

(1) * * *

* * * * * * *

(7) * * *

(8) PROPOSAL EVALUATION.—The Director shall—

(A) give consideration for the use of amounts in the Fund to improve the security of high value assets; and

(B) require that any proposal for the use of amounts in the Fund includes, as appropriate—

(i) a cybersecurity risk management plan; and

(ii) a supply chain risk assessment in accordance with section 1326 of title 41.

(c) * * *

(1) * * *

(2) * * *

(A) * * *

(i) addressing the greatest security, privacy, and operational risks, *including a consideration of the impact of high value assets;*

* * * * * * *

(5) * * *

(A) the Administrator of the Office of Electronic Government; [and]

(B) a senior official from the General Services Administration having technical expertise in information technology development, appointed by the Administrator, with the approval of the Director[.] *and*

(C) a senior official from the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, appointed by the Director.

(6) ADDITIONAL MEMBERS OF THE BOARD.—

(A) APPOINTMENT.—The other members of the Board [shall be—

[(i) 1 employee of the National Protection and Programs Directorate of the Department of Homeland Security, appointed by the Secretary of Homeland Security; and

(ii) [4 employees] *shall be 4 employees* of the Federal Government primarily having technical expertise in information technology development, financial man-

agement, cybersecurity and privacy, and acquisition, appointed by the Director.

* * * * * * *

○