Calendar No. 673

117TH CONGRESS *2d Session*	SENATE	REPORT 117–274

FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2021

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 2902

TO MODERNIZE FEDERAL INFORMATION SECURITY MANAGEMENT, AND FOR OTHER PURPOSES

DECEMBER 19, 2022.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE

39–010 WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
ALEX PADILLA, California
JON OSSOFF, Georgia

ROB PORTMAN, Ohio
RON JOHNSON, Wisconsin
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
JEFFREY D. ROTHBLUM, *Senior Professional Staff Member*
PAMELA THIESSEN, *Minority Staff Director*
SAM J. MULOPULOS, *Minority Deputy Staff Director*
WILLIAM H.W. MCKENNA, *Minority Chief Counsel*
CARA G. MUMFORD, *Minority Director of Governmental Affairs*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 673

117TH CONGRESS
2d Session

SENATE

REPORT
117–274

FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2021

DECEMBER 19, 2022.—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. 2902]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 2902), to modernize Federal information security management, 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. 2902, the *Federal Information Security Modernization Act of 2021* (FISMA 2021), 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 re-

port and respond to cyber attacks, codifies and expands security priorities such as zero trust architecture, and enhances logging and detection capabilities. FISMA 2021 also provides new operational authorities to bolster CISA's lead role in supporting agency information security programs, ensuring that CISA is the central point for reporting and help to remediate incidents and breaches on Federal networks.

II. Background and Need for the Legislation

The United States' Federal cybersecurity posture has left America's data at risk.[1] Despite reforms to Federal cybersecurity codified in FISMA 2014, Federal agencies continue to receive poor marks for cybersecurity.[2] Recent attacks, such as the SolarWinds breach, 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.[3]

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.[4] These hearings and report illuminated several themes that FISMA 2021 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;
- The importance of the National Cyber Director (NCD) and Cybersecurity and Infrastructure Security Agency (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 2021 addresses these issues by building on and updating FISMA 2014. The bill updates the law to recognize and clearly define the roles of two Federal entities that did not exist when FISMA 2014 was passed: 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. 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. They are also tasked with centralizing analysis of incident data, to re-

---

[1] Senate Committee on Homeland Security and Governmental Affairs, *Federal Cybersecurity: America's Data* Still *At Risk* (Aug. 2021) (S. Rept. 117–XX).

[2] *Id*.

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

[4] 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–XX); 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–XX); 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–XX); 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–XX); Senate Committee on Homeland Security and Governmental Affairs, *Federal Cybersecurity: America's Data Still At Risk* (Aug. 2021) (S. Rept. 117–XX).

duce the burden on each agency and enable Federal-wide analysis of cyber attacks.

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.[5] 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, only 3 major incidents were reported, and in FY 2020 only 6 major incidents were reported, with about 30,000 total agency incidents occurring in each of those two years.[6] 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.[7] FISMA 2021 attempts to address this issue by explicitly defining the thresholds for "major incidents" that need to be reported to Congress.

The major incident definition in FISMA 2021 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, while the FISMA 2021 language also includes cyber incidents that impact an agency's ability to deliver a critical service, that impact high value assets agencies, and require notification when sensitive agency information is exposed to a foreign entity. The major incident definition also changes the thresholds for reporting to Congress when personally identifiable information is breached, and 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.[8] 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.[9] During the SolarWinds compromise, some agencies declared major incidents to Congress, while others who were publicly reported to have been impacted, did not. Preliminary 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 cy-

---

[5] 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).

[6] 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)

[7] Senate Committee on Homeland Security and Governmental Affairs, *Federal Cybersecurity: America's Data* Still *At Risk* (Aug. 2021) (S. Rept. 117–XX)

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

[9] 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)

bersecurity incidents, for lack of any other mechanism to determine the full impact to the Federal government.[10]

FISMA 2021 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 also shifts existing agency annual FISMA reports to be every two years, and requires agencies move to automation for information sharing throughout the legislation.

Additionally, the Committee performed oversight over the Biden Administration's Executive Order 14028 on cybersecurity, including requirements for agencies to move to Zero Trust Architectures.[11] Several provisions of FISMA 2021 are based on that directive and other recent 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.[12]

III. Legislative History

Chairman Peters (D–MI) and Ranking Member Portman (R–OH) introduced S. 2902, the *Federal Information Security Modernization Act of 2021*, on September 29, 2021. The bill was referred to the Senate Committee on Homeland Security and Governmental Affairs. The Committee considered S. 2902 at a business meeting on October 6, 2021.

During the business meeting, a substitute amendment, as modified, was offered by Chairman Peters and Ranking Member Portman which made technical corrections, adjusted a number of activity deadlines throughout the text, updated the definition of "breach," updated the threshold for reporting breaches to Congress, updated the section on Zero Trust Architecture and least privilege principles, and removed several sections from the bill. The Peters-Portman substitute amendment, as modified, was adopted by unanimous consent, with Senators Peters, Carper, Hassan, Rosen, Padilla, Ossoff, Portman, Lankford, Romney, Scott, and Hawley present.

The Committee ordered the bill, as amended, reported favorably by voice vote with Senators Peters, Carper, Hassan, Rosen, Padilla, Ossoff, Portman, Lankford, Romney, Scott, and Hawley present.

---

[10] 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)

[11] Exec. Order No. 14028, 86 Fed. Reg. 26633 (May 12, 2021).

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

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

Section 1. Short title

This section designates the short title of the bill as the "Federal Information Security Modernization Act of 2021."

Section 2. Table of contents

This section contains the table of contents.

Section 3. Definitions

This section defines "additional cybersecurity procedure," "agency," "appropriate congressional committees," Director," "incident," "national security system," "penetration test," and "threat hunting."

TITLE I. UPDATES TO FISMA

Section 101. Title 44 amendments

This section amends several sections within title 44, U.S. Code.

- *Subsection (a)* amends U.S. Code sections in subchapter I of chapter 35 of title 44.
  - *(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) and the Director of the Cybersecurity and Infrastructure Security Agency (CISA) to develop policies, principles, standards, and guidelines on information confidentiality and security.
  - *(a)(2)* amends 44 U.S.C. § 3505. It includes the NCD and the Director of CISA on 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.
  - *(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)(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 Director of CISA.
- *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 "additional cybersecurity procedure," "high value asset," "major incident," "penetration test," and "shared service."
  - *(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 CISA as the lead cybersecurity entity for operational coordination and operational implementation across the Federal government, recognizes OMB as the leader for Federal cybersecu-

rity policy development and oversight, and recognizes the NCD as responsible for developing the U.S. Cybersecurity Strategy and advising the President on cybersecurity.

○ *(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 requires OMB to work with CISA and the NCD to oversee agency information security policies and practices, including overseeing agency compliance. It also requires OMB to work with CISA and NIST to promote the use of automation and least privilege principles to improve cybersecurity. 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 submit a report to Congress that includes the trends identified in the Federal risk assessment. This subsection also requires CISA to report to appropriate reporting entities, including Congress, within two days on the implementation by an agency of any binding operational or emergency directive issued by CISA to that agency.

○ *(c)(3)* amends 44 U.S.C. § 3554. This subsection requires agency heads to perform an ongoing and continuous agency risk assessment, specifies what must be included in that assessment, and requires that an update on that assessment to be provided to OMB, CISA, and the NCD. It requires agency heads to consult with OMB and CISA to evaluate whether additional cybersecurity procedures are required for individual information systems, provide those evaluations and implementation plans for any additional cybersecurity procedures to OMB, CISA, and the NCD, and ensure that those additional procedures are reflected in the risk-based cyber budget model. *(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. This subsection requires information security officers of component agencies to carry out various information security responsibilities and report to their designated senior information security officer and the Chief Information Officer of the component agency. *(c)(3)* also requires each agency to submit a biannual report summarizing its annual risk assessment, evaluating the effectiveness of cybersecurity policies, summarizing evaluations and implementation plans, and summarizing the status of remedial actions identified by the agency Inspector General, GAO, or any other source to OMB, DHS, relevant Congressional

committees, the NCD, and GAO. Finally, the subsection directs that, to the greatest extent practicable, those reports should be unclassified.

- *(c)(4)* amends 44 U.S.C. § 3555. This subsection changes the independent evaluations of agency information security programs and practices from yearly to biannual and instructs agencies, evaluators, Congressional committees, and any other recipients of the information from those audits to take steps to protect information that, if disclosed, could adversely affect information security. 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.
- *(c)(5)* amends 44 U.S.C. § 3556(a) to require the 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. This new subchapter contains new sections, discussed below:
  - § 3591 defines "appropriate reporting entities," "awardee," "contractor," "federal information," "federal information system," "intelligence community," "nationwide consumer reporting agency," "vulnerability disclosure," and "breach." It also imports definitions from sections § 3502 and § 3552.
  - § 3592 requires agency heads to expeditiously determine whether notice to individuals potentially impacted by a cybersecurity breach is appropriate and, if appropriate, notify 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 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. It also imposes documentary requirements on such a delay. 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.
  - § 3593 requires agencies to provide written notification to the appropriate reporting entities, and if practicable a briefing to Congress, within 72 hours after the agency has reasonable basis to conclude that a major inci-

dent occurred. It specifies the content of the report, and of a supplemental report required within 30 days after the written notification provided to the appropriate reporting entities is submitted, and requires the agency to provide an updated report if there is any significant change in the agency's understanding of the incident. The section also requires the agency, the NCD, and any other Federal entity deemed appropriate by the NCD to provide a briefing to Congress on the threat that caused the incident within seven days after the incident.

○ § 3594 requires agency heads to provide any information on any incident to CISA and OMB, and specifies the contents of that communication. It also requires each agency that has been the target of a major incident involving federal information in electronic medium or form, not involving a national security system, to consult with CISA regarding response, recovery, and mitigation.

○ § 3595 imposes responsibilities on Federal contractors and awardees who have been targets of cyber incidents or breaches to immediately report to the contracting or grantor agency immediate with respect to: Federal information collected, used, or maintained in connection with the contract, grant, or cooperative agreement; a Federal information system used or operated by the contractor or awardee in connection with the contract, grant, or cooperative agreement, or; it has received information from the agency it was not authorized to receive. In a major incident, the agency must consult with the contractor or awardee to comply with the requirements of §§ 3592, 3593, and 3594. If it is not a major incident, the agency, in consultation with the contractor or awardee, must comply with § 3594. This section becomes effective one year after enactment.

○ § 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. 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, and directs CISA and OMB to produce an annual report on federal incidents beginning not later than two years after enactment. 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, an annual report including data not provided to CISA that meets the requirements in this section. Finally, the section requires that information contained in the report must be anonymized to prevent identification of specific incidents

with specific agencies unless OMB and the impacted agency are consulted.

- § 3598 requires the Director of OMB, in coordination with the Director of CISA and the NCD, to issue guidance on the definition of "major incident" 180 days after the enactment of this bill. 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. This section also includes a requirement for OMB, CISA, the Privacy and Civil Liberties Oversight Board (PCLOB), and the Federal Trade Commission (FTC) to establish within 90 days of enactment of this legislation a risk-based framework to help agencies determine if an incident involving personally identifiable information could result in substantial harm, embarrassment or unfairness to an individual.

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

Section 102. 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. § 2(c)(4)(A)(ii). It directs the Director of CISA to coordinate with existing cybersecurity and governance frameworks, risk management best practices and prioritizing risk, impact, and consequences.
- *Subsection (b)* amends 40 U.S.C. § 11301. It prioritizes the funds in an agency's IT working capital fund to include improving cybersecurity and systems along with cost savings activities.
  - *Subsection (b)(1)(B)* requires agency CIOs to consult with necessary stakeholders, including the Director of CISA, when using funds affiliated with the IT working capital fund.
  - *Subsection (b)* also adds definitions of "Agency" and "High Value Asset". This amendment also requires the Director of OMB to advise agencies on the best utilization of the fund.
  - *Subsection (b)* also adds a senior official from CISA to the Technology Modernization Board.
- *Subsection (c)* 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.
  - *Subsection (c)* also adds data on costs, schedules, security and performance, for public availability.
  - This subsection requires the OMB to provide the NCD agency cybersecurity funding information as appropriate.
- *Subsection (d)* amends several sections of title 40, including 40 U.S.C. § 11315, by requiring the Chief Information Officers of component agency to report to their parent agency Chief Information Officer and the head of the component agency.
- *Subsection (e)* amends 40 U.S.C. § 11331. The head of every agency, in consultation with senior agency information security officers, must evaluate the need to employ (and, if

needed, actually employ) standards that are more stringent than those promulgated by OMB. Increased reporting requirements, stored data information, risk assessments, vulnerabilities, and threat hunting results are required to be maintained and coordinated with the Director of CISA.

- It also requires the Director of OMB to await public comment and consult with the Director of CISA, the Chief Information Officers Council, the Comptroller General of the United States, and the Council of Inspector Generals on Integrity and Efficiency (CIGIE), before promulgating or significantly modifying a proposed standard issued by the Director of NIST.
- It requires the Director of OMB to review the efficacy of the guidance and policy promulgated by OMB to reduce cybersecurity risks, including an assessment of the requirements on agencies to report to the Director and shall provide updated guidance based on that review every three years.
- OMB will also issue a public report within 30 days after the completion of that review specifying the guidance and policy currently in effect, the risk mitigation or other benefit offered by that guidance or policy, and a summary of any changes made by the review.
- It also requires OMB to report to the Senate Committee on Homeland Security and Governmental Affairs and the House Committee on Oversight and Reform on that review.

- It also requires the Director of NIST to develop and issue federal information system standards. The Director of NIST shall consider developing, in consultation with the Director of CISA and if appropriate and practical, specifications to enable an automated verification of the implementation of the controls described within the standards.

Section 103. Actions to enhance federal incident response

- *Subsection (a)* requires that CISA develop a plan for the analysis required under 44 U.S.C. 3597(b) 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 § 3594(a), § 3594(c), § 3595, and § 3596.
- *Subsection (c)* amends 5 U.S.C. § 552a(b), the "Privacy Act of 1974" to clarify when disclosure of information to another federal agency is warranted to facilitate a response to a cybersecurity incident, a federal agency may provide it after the head of the requesting agency has provided a written request to the agency specifying the particular portion of information necessary and for what purpose.

Section 104. Additional guidance to agencies on FISMA updates

This section requires the Director of OMB, in coordination with the Director of CISA, to issue guidance on:

- Performing the ongoing and continuous agency risk assessment required under law being amended by this Act;
- Implementing additional cybersecurity procedures;
- Establishing a process for providing a status of remediation to OMB and CISA.
- Interpretation of the definition of "high value asset";
- Coordination with agency OIGs to ensure understanding and application of agency policies for the purpose of agency OIG evaluations; and

Section 105. Agency requirements to notify private sector entities impacted by incidents

This section directs the Director of OMB to issue guidance that requires agencies to notify private sector entities of cybersecurity incidents impacting the sensitive information shared by that private sector entity with the agency or the systems used to transmit described information.

TITLE II. IMPROVING FEDERAL CYBERSECURITY

Section 201. Mobile security standards

This section requires an evaluation of mobile security standards.

- *Subsection (a)* requires OMB, within one year of enactment, to evaluate the mobile application security guidance promulgated by OMB and to issue guidance to secure mobile devices for every agency.
- *Subsection (b)* specifies the contents of that guidance, including conducting an inventory of mobile devices and vulnerabilities, for every federal agency, and requires that every agency continuously evaluate those vulnerabilities.
- *Subsection (c)* requires OMB, in coordination with CISA to issue guidance on how to share the inventory in subsection (b) with CISA.
- *Subsection (d)* requires OMB in coordination with CISA to provide briefings to Congress on the guidance in subsection (b).

Section 203. Data and logging retention for incident response

This section requires certain data and log retention elements for Federal agencies.

- *Subsection (a)* requires the Director of CISA, in consultation with the Attorney General, to submit recommendations not later than two years after enactment to OMB on how to log events on agency systems and how to retain other relevant network and systems data.
- *Subsection (b)* specifies the contents of those recommendations.
- *Subsection (c)* requires OMB, as determined appropriate by the Director of OMB and in consultation with the Director of CISA and the Attorney General, to update guidance for agencies regarding requirement for logging, log retention, log management, sharing of log data, and any other appropriate log-

ging activity, within 90 days after receiving the recommendations.

Section 203. CISA agency advisors

This section creates a liaison between CISA and each agency. Within 120 days after enactment of FISMA 2021, 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 an advisor, and stipulates that the advisor shall not be a contractor but may be assigned to multiple senior agency information security officers.

Section 204. Federal penetration testing policy

Subsection (a) amends 44 U.S.C. chapter 35 by adding section 3559A, which allows CISA to enter into rules of engagement contracts with agencies for penetration testing. Requires OMB within 180 days to issue guidance requiring agencies to use penetration testing on agency systems when and where appropriate. 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.

Section 205. Ongoing threat hunting program

This section establishes a Threat Hunting Program under CISA within 540 days adding to the additional cybersecurity procedures under section 3554 of title 44, United States Code. The section also requires a plan from the Director of CISA within 180 days that details how CISA will collect and analyze appropriate agency data, resources required to support the program, and consultation with agency heads on how the program will complement or improve cybersecurity efforts at individual agencies.

Section 206. Codifying vulnerability disclosure programs

This section requires that agencies create and follow a vulnerability disclosure program. Agencies will also disclose to CISA any discovered or not publicly known vulnerabilities in agency information systems or commercially used systems. OMB shall also submit a report 90 days after the date of enactment, and every three years thereafter on the status of the use of vulnerability disclosure policies.

Section 207. Implementing presumption of compromise and least privilege principles

This section requires OMB, in consultation with CISA and NIST and not later than 1 year after enactment, to provide an update to Congress on progress in increasing the internal defenses of agency

systems. This section also requires agencies to submit to OMB a progress report on the implementation of information security programs based on the presumption of compromise and lease privilege principles.

Section 208. Automation Reports

This section requires an OMB Report of the use of automation in 44 U.S.C. 3554(b) to Congress within 180 days after the date of enactment, and also requires a GAO Report detailing the use of automation and machine readable data cross the Government for cybersecurity purposes within one year of enactment.

Section 209. Extension of Federal Acquisition Security Council

This section extends the sunset on the Federal Acquisition Security Council to December 31, 2026.

Section 210. 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).

TITLE III. RISK-BASED BUDGET MODEL

Section 301. Definitions

This section defines certain terms, including "appropriate congressional committees," "covered agency," "director," "information technology," and "risk-based budget."

Section 302. Establishment of risk-based model

This section requires OMB, in consultation with CISA, the NCD, and in coordination with NIST, to develop a standard model for creating a risk-based budget for cybersecurity spending within one year after the first publication of the President's budget following enactment of this act.

- It specifies the content of this model, requires triennial updates to the model by OMB, and mandates publication of the model on the OMB website.
- It also requires OMB to report annually on the development of the model from passage of this act until completion of the model.
- This section also requires that every agency, within two years after publication of the model, use the model to develop their annual cybersecurity and information technology budget request.
- It also includes an assessment of agency implementation of risk-based budget models in the independent evaluation under 44 U.S.C. 3555, and requires a GAO report submitted to appropriate congressional committees evaluating the development, implementation, and success of the risk-based budgets developed by agencies.

TITLE IV. PILOT PROGRAMS TO ENHANCE FEDERAL CYBERSECURITY

Section 401. Active cyber defense study

This section defines "active defense technique" and authorizes an active cyber defense pilot program.

- Subsection (a) defines the term "active defense technique."
- Subsection (b) requires the Director of CISA, in coordination with OMB, to perform a study on the use of active defense techniques to enhance the security of agencies. The study shall include a legal review on the use of active defense techniques; efficacy of selection of active defense techniques and efficacy factors; and development of a framework to use different techniques by agencies.

Section 402. Security operations center as a service pilot

This section creates a pilot program allowing CISA to create and operate a security operation center on behalf of other federal agencies.

- Subsection (a) establishes that the purpose of this section is for CISA to run a security operation center on behalf of another agency, alleviating the need to duplicate this function at every agency, and empowering a greater centralized cybersecurity capability.
- Subsection (b) requires the Director of CISA to develop a plan within 1 year to establish a centralized Federal security operation center.
- Subsection (c) requires certain elements of the plan, including consideration for collecting, organizing, and analyzing agency information system data in real time; staff and resource the center, and enter into agreements and governance plans with agencies.
- Subsection (d) directs the Director of CISA, in consultation with the Director of OMB, to initiate this pilot program with not less than two federal agencies for a one-year agreement to offer a security operations center as a shared service.
- Subsection (e) requires CISA to report to appropriate Congressional Committees not later than 260 days after the enactment of this act, to report the parameters and conditions of any one-year agreements signed to date.

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

U.S. Congress,
Congressional Budget Office,
Washington, DC, November 9, 2022.

Hon. Gary C. Peters,
Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has prepared the enclosed table summarizing estimated budgetary effects and mandates information for some of the legislation that has been ordered reported by the Senate Committee on Homeland Security and Governmental Affairs during the 117th Congress.

If you wish further details, we will be pleased to provide them. The CBO staff contact for each estimate is listed on the enclosed table.

Sincerely,

Phillip L. Swagel,
Director.

Enclosure.

Summary Estimates of Legislation Ordered Reported

The Congressional Budget Act of 1974 requires the Congressional Budget Office, to the extent practicable, to prepare estimates of the budgetary effects of legislation ordered reported by Congressional authorizing committees. In order to provide the Congress with as much information as possible, the attached table summarizes information about the estimated direct spending and revenue effects of some of the legislation that has been ordered reported by the Senate Committee on Homeland Security and Governmental Affairs during the 117th Congress. The legislation listed in this table generally would have small effects, if any, on direct spending or revenues, CBO estimates. Where possible, the table also provides information about the legislation's estimated effects on spending subject to appropriation and on intergovernmental and private-sector mandates as defined in the Unfunded Mandates Reform Act.

ESTIMATED BUDGETARY EFFECTS AND MANDATES INFORMATION

Bill Number	Title	Status	Last Action	Budget Function	Direct Spending, 2023–2032	Revenues, 2023–2032	Spending Subject to Appropriation, 2023–2027	Pay-As-You-Go Procedures Apply?	Increases On-Budget Deficits Beginning in 2033?	Mandates	Contact
S. 2902	Federal Information Security Modernization Act of 2021	Ordered reported	10/06/21	800	Between zero and $500,000	0	Not estimated	Yes	No	No	Matthew Pickford

S. 2902 would amend federal information security policies and authorize pilot programs to enhance federal cybersecurity. CBO estimates that enacting S. 2902 would have an insignificant effect on direct spending and no effect on revenues over the 2023–2032 period. CBO has not estimated the discretionary costs of implementing the bill. The bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act.

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 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**[**.**]***; and*

(13) to another agency in furtherance of a response to an incident (as defined in section 3552 of title 44) and pursuant to the information sharing requirements in section 3594 of title 44 if the head of the requesting agency has made a written request to the agency that maintains the record specifying the particular portion desired and the activity for which the record is sought.

* * * * * * *

TITLE 5—APPENDIX

* * * * * * *

INSPECTOR GENERAL ACT OF 1978

* * * * * * *

SEC. 11. 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, United States Code; and

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

* * * * * * *

TITLE 10—ARMED FORCES

* * * * * * *

Subtitle A—General Military Law

* * * * * * *

PART IV—SERVICE, SUPPLY, AND PROCUREMENT

* * * * * * *

CHAPTER 131—PLANNING AND COORDINATION

* * * * * * *

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

* * * * * * *

(i) * * *

(1) * * *

* * * * * * *

(8) NATIONAL SECURITY SYSTEM.—The term "national security system" has the meaning given that term in **[**section 3552(b)(6)(A)**]** *section 3552(b)(9)(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.

* * * * * * *

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)] *section 3552(b)* of title 44, United States Code.

* * * * * * *

SEC. 2224. DEFENSE INFORMATION ASSURANCE PROGRAM

* * * * * * *

STRATEGY ON COMPUTER SOFTWARE ASSURANCE

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

* * * * * * *

CHAPTER 137—PROCUREMENT GENERALLY

* * * * * * *

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

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

* * * * * * *

SEC. 2339a. 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 15—COMMERCE AND TRADE

* * * * * * *

CHAPTER 7—NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

* * * * * * *

SEC. 278g-3. COMPUTER STANDARDS PROGRAM

(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)(5)] *section 3552(b)* of title 44);

* * * * * * *

(d) * * *

(1) * * *

(2) * * *

(3) conduct research and analysis—

(A) to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security;

(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 under§section 3553 or 3554 of title 44, 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) * * *

(3) the term "information technology" has the same meaning as provided in [section 3502(8)] *section 3552(b)* of such title;

(4) * * *

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

SEC. 278g–3a. 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.

* * * * * * *

CHAPTER 81—HIGH–PERFORMANCE COMPUTING

* * * * * * *

Subchapter II—Agency Activities

* * * * * * *

SEC. 5527. 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)(9)(A)(i)* of title 44.

* * * * * * *

TITLE 31—MONEY AND FINANCE

* * * * * * *

Subtitle II—The Budget Process

* * * * * * *

CHAPTER 11—THE BUDGET AND FISCAL, BUDGET, AND PROGRAM INFORMATION

* * * * * * *

SEC. 1105. BUDGET CONTENTS AND SUBMISSION TO CONGRESS.

(a) * * *

* * * * * * *

(35)(A)(i) a detailed, separate analysis, by budget function, [by agency, and by initiative area (as determined by the administration)] *and by agency* for the prior fiscal year, the current fiscal year, the fiscal years for which the budget is submitted, and the ensuing fiscal year identifying the amounts of gross and net appropriations or obligational authority and outlays that contribute to cybersecurity, with separate displays for mandatory and discretionary amounts, including

(I) * * *

(II) * * *

(III) the most recent risk assessment and summary of cybersecurity needs in each initiative area (as determined by the administration); [and]

(IV) * * *

(V) a validation that the budgets submitted were developed using a risk-based methodology; and

(VI) a report on the progress of each agency on closing recommendations identified under the independent evaluation required by section 3555(a)(1) 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. 11301. RESPONSIBILITY OF DIRECTOR

* * * * * * *

STATUTORY NOTES AND RELATED SUBSIDIARIES

* * * * * * *

GSA MODERNIZATION CENTERS OF EXCELLENCE PROGRAM

Pub. L. 116–194, 2, Dec. 3, 2020, 134 Stat. 981, provided that:
(a) * * *
(b) * * *
(c) RESPONSIBILITIES.—The Program shall have the following responsibilities:
(1) * * *
(2) * * *
(3) * * *
(4) * * *
(A) * * *
(i) * * *
(ii) a cybersecurity and governance framework the promotes industry and government risk management best practice approaches, prioritizing efforts based on risk, impact, and consequences**[**.**]**, *which shall be provided in coordination with the director of the Cybersecurity and Infrastructure Security Agency.*

* * * * * * *

MODERNIZING GOVERNMENT TECHNOLOGY

Pub. L. 115—91, div. A, title X, subtitle G, Dec. 12, 2017, 131 Stat. 1586, provided that:

* * * * * * *

SEC. 1077. ESTABLISHMENT OF AGENCY INFORMATION TECHNOLOGY SYSTEMS MODERNIZATION AND WORKING CAPITAL FUNDS.

(a) * * *
(b) * * *
(1) * * *

* * * * * * *

(5) PRIORITIZATION OF FUNDS.—The head of each covered agency—
(A) shall prioritize funds within the IT working capital fund of the covered agency to be used initially *for improving the cybersecurity of systems and* cost savings activities approved by the Chief Information Officer of the covered agency; and

(B) * * *

(6) * * *

(7) AGENCY [CIO] *CIO* responsibilities.—

(A) CONSIDERATION OF GUIDANCE.—In evaluating projects to be funded by the IT working capital fund of a covered agency, the Chief Information Officer of the covered agency shall consider, to the extent applicable, guidance issued [under section 1094(b)(1)] *by the Director* to evaluate applications for funding from the Fund that include factors including a strong business case, technical design, consideration of commercial off-the-shelf products and services, procurement strategy (including adequate use of rapid, iterative software development practices) and program management.

(B) CONSULTATION.—*In using funds under paragraph (3)(A), the Chief Information Officer of the covered agency shall consult with the necessary stakeholders to ensure the project appropriately addresses cybersecurity risks, including the Director of the Cybersecurity and Infrastructure Security Agency as appropriate.*

* * * * * * *

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 a cybersecurity plan, including a supply chain risk management plan, to be reviewed by the members of the Technology Modernization Board described in subsection (c)(5)(C).

(c) * * *

(1) * * *

(2) RESPONSIBILITIES.—The responsibilities of the Board are—

(A) to provide input to the Director for the development of processes for agencies to submit modernization proposals to the Board and to establish the criteria by which those proposals are evaluated, which shall include—

(i) addressing the greatest security, privacy, and operational risks, *including a consideration of the impact of high value assets;*

(ii) * * *

* * * * * * *

(5) PERMANENT MEMBERS.—The permanent members of the Board shall be—

(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 [now Cybersecurity and Infrastructure Security Agency] 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 management, cybersecurity and privacy, and acquisition, appointed by the Director.

* * * * * * *

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.

(c) USE OF BUDGET PROCESS.—

(1) * * *

(2) * * *

(3) PUBLIC AVAILABILITY.—

(A) IN GENERAL.—The Director shall make available to the public a list of each major information technology investment, without regard to whether the investments are for new information technology acquisitions or for operations and maintenance of existing information technology, [including data] *which shall—*

(i) include data on cost, schedule[, and performance] *security, and performance; and*

(ii) specifically denote cybersecurity funding under the risk-based cyber budget model developed pursuant to section 3553(a)(7) of title 44.

(B) * * *

(i) * * *
(ii) * * *
(iii) The Director shall provide to the National Cyber Director any cybersecurity funding information described in subparagraph (A)(ii) that is provided to the Director under clause (ii) of this subparagraph.
(4) * * *
(A) * * *
(B) *not later than 30 days after the date on which the review under subparagraph (A) is completed,* the Administrator of the Office of Electronic Government shall communicate the results of the review under subparagraph (A) to—

* * * * * * *

(f) USE OF BEST PRACTICES IN ACQUISITIONS.—The Director shall encourage the **[**heads of the executive agencies to develop**]** *heads of executive agencies to—*

*(1) develop and use the best practices in the acquisition of information technology***[***.***]****; and*

(2) consult with the Director of the Cybersecurity and Infrastructure Security Agency for the development and use of supply chain security best practices.

(g) * * *

(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;

* * * * * * *

(5) * * *
(A) * * *
(B) * * *

(i) recommending a reduction or an increase in the amount for information resources that the head of the executive agency proposes for the budget submitted to Congress under section 1105(a) of title 31, *while taking into account the risk-based cyber budget model developed pursuant to section 3553(a)(7) of title 44;*

* * * * * * *

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 under section 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. 11315. AGENCY CHIEF INFORMATION OFFICER

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

(d) COMPONENT AGENCY CHIEF INFORMATION OFFICERS.—The Chief Information Officer or an equivalent official of a component agency shall report to—

(1) the Chief Information Officer designated under section 3506(a)(2) of title 44 or an equivalent official of the agency of which the component agency is a component; and

(2) the head of the component agency.

* * * * * * *

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*.—

* * * * * * *

Subchapter III—Other Responsibilities

* * * * * * *

SEC. 11331. RESPONSIBILITIES FOR FEDERAL INFORMATION SYSTEMS STANDARDS

(a) DEFINITION.—In this section, the term "information security" has the meaning given that term in section [3532(b)(1)] *section 3552(b)* of title 44.

(b) * * *

(1) * * *

(A) REQUIREMENT.—Except as provided under paragraph (2), the Director of the Office of Management and Budget shall, on the basis of proposed standards developed by the National Institute of Standards and Technology pursuant to paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)) and [in consultation] *in coordination with* [the Secretary of Homeland Security] *the Director of the Cybersecurity and Infrastructure Security Agency,* promulgate information security standards pertaining to Federal information systems.

* * * * * * *

[(c) APPLICATION OF MORE STRINGENT STANDARDS.—The head of an agency may employ standards for the cost-effective information security for all operations and assets within or under the supervision of that agency that are more stringent than the standards promulgated by the Director under this section, if such standards—

(1) contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Director; and

(2) are otherwise consistent with policies and guidelines issued under section 3533 1 of title 44.]

(C) APPLICATION OF MORE STRINGENT STANDARDS.—

(1) IN GENERAL.—The head of an agency shall—

(A) evaluate, in consultation with the senior agency information security officers, the need to employ standards for cost-effective, risk-based information security for all systems, operations, and assets within or under the supervision of the agency that are more stringent than the standards promulgated by the Director under this section, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Director; and

(B) to the greatest extent practicable and if the head of the agency determines that the standards described in subparagraph (A) are necessary, employ those standards.

(2) EVALUATION OF MORE STRINGENT STANDARDS.—In evaluating the need to employ more stringent standards under paragraph (1), the head of an agency shall consider available risk information, such as—

(A) the status of cybersecurity remedial actions of the agency;

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

(C) incident information of the agency;

(D) information from

(i) penetration testing performed under section 3559A of title 44; and

(ii) information from the vulnerability disclosure program established under section 3559B of title 44;

(E) agency threat hunting results under section 205 of the Federal Information Security Modernization Act of 2021;

(F) Federal and non-Federal threat intelligence;

(G) data on compliance ith standards issued under this section;

(H) agency system risk assessments performed under section 3554(a)(1)(A) of title 44; and

(I) any other information determined relevant by the head of the agency.

(d) * * *

(1) * * *

(2) [NOTICE AND COMMENT] *CONSULTATION, NOTICE, AND COMMENT.*—A decision by the Director to *promulgate* significantly modify, or not promulgate, a proposed standard submitted to the Director by the National Institute of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), [shall be made after the public is given an opportunity to comment on the Director's proposed decision.] *shall be made—*

(A) for a decision to significantly modify or not promulgate such a proposed standard, after the public is given an opportunity to comment on the Director's proposed decision;

(B) in consultation with the Chief Information Officers Council, the Director of the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, the Comptroller General of the United States, and the Council of the Inspectors General on Integrity and Efficiency;

(C) considering the Federal risk assessments performed under section 3553(i) of title 44; and

(D) considering the extent to which the proposed standard reduces risk relative to the cost of implementation of the standard.

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

(1) CONDUCT OF REVIEW.—

(A) IN GENERAL.—Not less frequently than once every 3 years, the Director of the Office of Management and Budget, in consultation with the Chief Information Officers Council, the Director of the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, the Comptroller General of the United States, and the Council of the Inspectors General on Integrity and Efficiency shall review the efficacy of the guidance and policy promulgated by the Director in reducing cybersecurity risks, including

an assessment of the requirements for agencies to report information to the Director, and determine whether any changes to that guidance or policy is appropriate.

(B) FEDERAL RISK ASSESSMENTS.—In conducting the review described in subparagraph (A), the Director shall consider the Federal risk assessments performed under section 3553(i) of title 44.

(2) UPDATED GUIDANCE.—Not later than 90 days after the date on which a review is completed under paragraph (1), the Director of the Office of Management and Budget shall issue updated guidance or policy to agencies determined appropriate by the Director, based on the results of the review.

(3) PUBLIC REPORT.—Not later than 30 days after the date on which a review is completed under paragraph (1), the Director of the Office of Management and Budget shall make publicly available a report that includes—

(A) an overview of the guidance and policy promulgated under this section that is currently in effect;

(B) the cybersecurity risk mitigation, or other cybersecurity benefit, offered by each guidance or policy document described in subparagraph (A); and

(C) a summary of the guidance or policy to which changes were determined appropriate during the review and what the changes are anticipated to include.

(4) CONGRESSIONAL BRIEFING.—Not later than 30 days after the date on which a review is completed under paragraph (1), the Director shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives a briefing on the review.

(f) AUTOMATED STANDARD IMPLEMENTATION VERIFICATION.—When the Director of the National Institute of Standards and Technology issues a proposed standard pursuant to paragraphs (2) and (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, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, specifications to enable the automated verification of the implementation of the controls within the standard

* * * * * * *

TITLE 41—PUBLIC CONTRACTS

* * * * * * *

Subtitle I—Federal Procurement Policy

* * * * * * *

Division B—Office of Federal Procurement Policy

* * * * * * *

CHAPTER 13—ACQUISITION COUNCILS

* * * * * * *

Subchapter III—Federal Acquisition Supply Chain Security

* * * * * * *

SEC. 1328. TERMINATION

This subchapter shall terminate on [the date that is 5 years after the date of the enactment of the Federal Acquisition Supply Chain Security Act of 2018] December 31, 2026.

* * * * * * *

TITLE 44—PUBLIC BUILDINGS, PROPERTY, AND WORKS

* * * * * * *

CHAPTER 35—COORDINATION OF FEDERAL INFORMATION POLICY

Sec.
3501. Purposes

* * * * * * *

Subchapter II—Federal Information Policy

3552. Definitions
[3553. Authority and functions of the Director and the Secretary]
3553. Authority and functions of the Director and the Director of the Cybersecurity and Infrastructure Security Agency.
3554. Federal agency responsibilities.
[3555. Annual independent evaluation.]
3555. Independent evaluation.

* * * * * * *

3559A. Federal penetration testing.
3559B. Federal vulnerability disclosure programs.

* * * * * * *

Subchapter IV—Federal System Incident Response

3591. Definitions.
3592. Notification of breach.
3593. Congressional and Executive Branch reports.
3594. Government information sharing and incident response.
3595. Responsibilities of contractors and awardees.
3596. Training.
3597. Analysis and report on Federal incidents.
3598. Major incident definition.

* * * * * * *

Subchapter I—Federal Information Policy

SEC. 3501. PURPOSES

* * * * * * *

INFORMATION SECURITY RESPONSIBILITIES OF CERTAIN AGENCIES

Pub. L. 107–347, title III, 301(c)(1)(A), Dec. 17, 2002, 116 Stat. 2955, provided that: "Nothing in this Act [see Tables for classifica-

tion] (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)] *section 3552(b)* of title 44, United States Code."

* * * * * * *

SEC. 3504. AUTHORITY AND FUNCTIONS OF DIRECTOR

(a)(1) * * *

(A) * * *

(B) provide direction and oversee—

(i) * * *

* * * * * * *

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

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

(vi) in consultation with the National Cyber Director and the Director of the Cybersecurity and Infrastructure Security Agency, 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) with respect to information collected or maintained by or for agencies—

(A) develop and oversee the implementation of policies, principles, standards, and guidelines on privacy, confidentiality, disclosure, and sharing of the information; and

(B) in consultation with the National Cyber Director and the Director of the Cybersecurity and Infrastructure Security Agency, develop and oversee policies, principles, standards, and guidelines on security of the information; and

(h) * * *

(1) in consultation with *the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director*, the Director of the National Institute of Standards and Technology, and the Administrator of General Services—

(A) develop and oversee the implementation of policies, principles, standards, and guidelines for information technology *security and* functions and activities of the Federal Government, including periodic evaluations of major information systems; and

* * * * * * *

SEC. 3505. ASSIGNMENT OF TASKS AND DEADLINES

(a) * * *

* * * * * * *

(c) * * *

(1) * * *

(2) * * *
(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.

* * * * * * *

[(c) Inventory of Information Systems.—(1) The head of each agency shall develop and maintain an inventory of the information systems (including 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.]

* * * * * * *

SEC. 3506. FEDERAL AGENCY RESPONSIBILITIES

(a) * * *
(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;

* * * * * * *

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 or cybersecurity to the Director of the Cybersecurity and Infrastructure Security Agency.

[(c)**]** *(d)* COMPARABLE TREATMENT.—Notwithstanding any other provision of law, the Director shall treat or review a rule or order prescribed or proposed by the Director of the Bureau of Consumer Financial Protection on the same terms and conditions as apply to any rule or order prescribed or proposed by the Board of Governors of the Federal Reserve System.

* * * * * * *

Subchapter II—Information Security

SEC. 3551. PURPOSES

The purposes of this subchapter are to—

(1) * * *

(2) * * *

(3) recognize the role of the Cybersecurity and Infrastructure Security Agency as the lead entity for operational cybersecurity coordination across the Federal Government;

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

[(4)**]** *(5)* provide a mechanism for improved oversight of Federal agency information security programs, including through automated security tools to continuously **[**diagnose and improve**]** *integrate, deliver, diagnose, and improve security*;

[(5)**]** *(6)* 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)**]** *(7)* recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products**[**.**]***;*

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

(9) 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

(10) recognize that—

(A) a holistic Federal cybersecurity model is necessary to account for differences between the missions and capabilities of agencies; and

(B) in accounting for the differences described in subparagraph (A) and ensuring overall Federal cybersecurity—

(i) the Office of Management and Budget is the leader for policy development and oversight of Federal cybersecurity;

(ii) the Cybersecurity and Infrastructure Security Agency is the leader for implementing operations at agencies; and

(iii) the National Cyber Director is responsible for developing the overall cybersecurity strategy of the United States and advising the President on matters relating to cybersecurity.

* * * * * * *

SEC. 3552. DEFINITIONS

(a) * * *

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

(1) The term 'additional cybersecurity procedure' means a process, procedure, or other activity that is established in excess of the information security standards promulgated under section 11331(b) of title 40 to increase the security and reduce the cybersecurity risk of agency systems.

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

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

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

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

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

(7) The term 'high value asset' means information or an information system that the head of an agency determines so critical to the agency that the loss or corruption of the information or the loss of access to the information system would have a serious impact on the ability of the agency to perform the mission of the agency or conduct business.

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

[(6)**]** *(9)* * * *

(10) The term 'penetration test' means a specialized type of assessment that—

(A) is conducted on an information system or a component of an information system; and

(B) emulates an attack or other exploitation capability of a potential adversary, typically under specific constraints, in order to identify any vulnerabilities of an information

system or a component of an information system that could be exploited.

[(7)] *(11)* * * *

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

* * * * * * *

SEC. 3553. [AUTHORITY AND FUNCTIONS OF THE DIRECTOR AND THE SECRETARY] *AUTHORITY AND FUNCTIONS OF THE DIRECTOR AND THE DIRECTOR OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY*

(a) * * *

(1) *in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director*, developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards promulgated under section 11331 of title 40;

* * * * * * *

(5) overseeing, *in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director*, agency compliance with the requirements of this subchapter and section 1326 of title 41, including through any authorized action under section 11303 of title 40, to enforce accountability for compliance with such requirements; [and]

(6) * * *

(7) developing a standard risk-based budget model to inform Federal agency cybersecurity budget development; and

(8) promoting, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency 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 to improve resiliency and timely response actions to incidents on Federal systems.

(b) [SECRETARY] CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.—[The Secretary, in consultation with the Director] *The Director of the Cybersecurity and Infrastructure Security Agency, 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 title*;

(B) * * *

(C) * * *

(D) other operational requirements as [the Director or Secretary] *the Director of the Cybersecurity and Infrastructure Security Agency*, in consultation with the Director, may determine necessary;

(3) * * *

(4) * * *

(5) [coordinating] *leading the coordination of* Government-wide efforts on information security policies and practices, including consultation with the Chief Information Officers Council established under section 3603 and the Director of the National Institute of Standards and Technology;

(6) * * *

(7) * * *

(8) upon request by an agency, and at [the Secretary's discretion] *the Director of the Cybersecurity and Infrastructure Security Agency's discretion*, with or without reimbursement

(A) * * *

(B) deploying, operating, and maintaining secure technology platforms and tools, including networks and common business applications, for use by the agency to perform agency functions, including collecting, maintaining, storing, processing, disseminating, and analyzing information; [and]

(9) performing penetration testing with or without advance notice to, or authorization from, agencies, to identify vulnerabilities within Federal information systems; and

[(9)] *(10)* other actions [as the Director or the Secretary, in consultation with the Director,] *as the Director of the Cybersecurity and Infrastructure Security Agency* may determine necessary to carry out this subsection.

(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 on the effectiveness of information security policies and practices during the preceding year, including—

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

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

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

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

(4) a summary of each assessment of Federal risk posture performed under subsection (i);

(5) an assessment of agency compliance with data breach notification policies and procedures issued by the Director[.]; and

(6) an assessment of—

(A) Federal agency implementation of the model required under subsection (a)(7);

(B) how cyber vulnerabilities of Federal agencies changed from the previous year; and

(C) whether the model mitigates the cyber vulnerabilities of the Federal Government;

* * * * * * *

(h) * * *

(i) FEDERAL RISK ASSESSMENTS.—On an ongoing and continuous basis, the Director of the Cybersecurity and Infrastructure Security Agency shall perform assessments of 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 those assessments including—

(1) the status of agency cybersecurity remedial actions 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 threat intelligence;

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

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

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

[(i)**]** *(j)* 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**]** *that includes a summary of*

(1) 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**[**.**]**; and

(2) the trends identified in the Federal risk assessment performed under subsection (i).

[(j)**]** *(k)* * * *

[(k)**]** *(l)* * * *

[(l)**]** *(m)* * * *

(n) BINDING OPERATIONAL DIRECTIVES.—If the Director of the Cybersecurity and Infrastructure Security Agency issues a binding operational directive or an emergency directive under this section, not later than 2 days after the date on which the binding operational directive requires an agency to take an action, the Director of the Cybersecurity and Infrastructure Security Agency shall provide to the appropriate reporting entities the status of the implementation of the binding operational directive at the agency.

* * * * * * *

SEC. 3554. FEDERAL AGENCY RESPONSIBILITIES

(a) * * *

(1) be responsible for—

(A) on an ongoing and continuous basis, performing agency system risk assessments that—

(i) identify and document the high value assets of the agency using guidance from the Director;

(ii) evaluate the data assets inventoried under section 3511 of title 44 for sensitivity to compromises in confidentiality, integrity, and availability;

(iii) identify agency systems that have access to or hold the data assets inventoried under section 3511 of title 44;

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

(v) evaluate 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;

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

(vii) assess 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 conducted under subparagraph (A), providing, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, information* security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

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

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

(iii) policies and procedures issued by the Director;

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

(v) emergency directives issued by the Secretary under section 3553(h); and

(vi) responsibilities relating to assessing and avoiding, mitigating, transferring, or accepting supply chain risks under section 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 performed under subparagraph (A)—

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

(ii) on a periodic basis, as determined by guidance issued by the Director but not less frequently than annually, to—

(I) the Director;

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

(III) the National Cyber Director;

(F) in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and not less frequently than once every 3 years, performing an evaluation of whether additional cybersecurity procedures are appropriate for securing a system of, or under the supervision of, the agency, which shall—

(i) be completed considering the agency system risk assessment performed under subparagraph (A); and

(ii) include a specific evaluation for high value assets;

(G) not later than 30 days after completing the evaluation performed under subparagraph (F), providing the evaluation and an implementation plan, if applicable, for using additional cybersecurity procedures determined to be appropriate to—

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

(ii) the Director; and

(iii) the National Cyber Director; and

(H) if the head of the agency determines there is need for additional cybersecurity procedures, ensuring that those additional cybersecurity procedures are reflected in the budget request of the agency in accordance with the risk-based cyber budget model developed pursuant to section 3553(a)(7);

(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 performed under paragraph (1)(A)*;

(B) determining the levels of information security appropriate to protect such information and information systems [in accordance with standards] *in accordance with—*

(i) *standards* promulgated under section 11331 of title 40, for information security classifications and related requirements;

(ii) the evaluation performed under paragraph (1)(F); and

(iii) the implementation plan described in paragraph (1)(G);

(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) * * *

(i) * * *

(ii) * * *

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

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

(v) ensure that—

(I) senior agency information security officers of component agencies carry out responsibilities under this subchapter, as directed by the senior agency information security officer of the agency or an equivalent official; and

(II) senior agency information security officers of component agencies report to—

(aa) the senior information security officer of the agency or an equivalent official; and

(bb) the Chief Information Officer of the component agency or an equivalent official;

* * * * * * *

(5) ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head *and the Director of the Cybersecurity and Infrastructure Security Agency* on the effectiveness of the agency information security program, including progress of remedial actions;

(6) * * *

(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) pursuant to subsection (a)(1)(A), performing ongoing and continuous agency system risk assessments, which may include using guidelines 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;]

(B) comply with the risk-based cyber budget model developed pursuant to section 3553(a)(7);

(C) * * *

(D) * * *

(i) * * *

(ii) * * *

(iii) binding operational directives and emergency directives promulgated by the Director of the Cybersecurity and Infrastructure Security Agency under section 3553;

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

(I) the agency risk assessment performed under subsection (a)(1)(A); and

(II) the determinations of applying more stringent standards and additional cybersecurity procedures pursuant to section 11331(c)(1) of title 40; and

[(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) a process for [planning, implementing, evaluating, and documenting] *planning and implementing and, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, evaluating and documenting* remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

(7) a process for providing the status of every remedial action and known system vulnerability 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 title; and

[(iii)] *(iv)* notifying and consulting with, as appropriate

(I) law enforcement agencies [and relevant offices of inspectors general] and Offices of General Counsel;

(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 Affairs and the Committee on Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General a report on the adequacy and effectiveness of information security policies, procedures, and practices, including—

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

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

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

(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) BIANNUAL REPORT.—Not later than 2 years after the date of enactment of the Federal Information Security Modernization Act of 2021 and not less frequently than once every 2 years thereafter, using the continuous and ongoing agency system risk assessment under subsection (a)(1)(A), the head of each agency shall submit to the Director, the Director of the Cybersecurity and Infrastructure Security Agency, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, the appropriate authorization and appropriations committees of Congress, the National Cyber Director, and the Comptroller General of the United States a report that—

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

(C) summarizes the evaluation and implementation plans described in subparagraphs (F) and (G) of subsection (a)(1) and whether those evaluation and implementation plans call for the use of additional cybersecurity procedures determined to be appropriate by the agency; and

(D) 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.

(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 a classified annex.

(3) ACCESS TO INFORMATION.—The head of an agency shall ensure that, to the greatest extent practicable, information is included in the unclassified form of the report submitted by the agency under paragraph (2)(A).

(4) 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)**]** *(5)* 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.*

(d) PERFORMANCE PLAN.—

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

(A) * * *

(B) * * *

(2) The description under paragraph (1) *and the risk-based budget model required under section 3553(a)(7)* shall be based on the risk assessments required under subsection (b)(1).

SEC. 3555. [ANNUAL INDEPENDENT] INDEPENDENT EVALUATION.

(a) IN GENERAL.—

(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) Each evaluation under this section shall include—

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

(B) an assessment of the effectiveness of the information security policies, procedures, and practices of the agency; **[**and**]**

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

(D) an assessment of how the agency implemented the risk-based budget model required under section 3553(a)(7) and an evaluation of whether the model mitigates agency cyber vulnerabilities.

(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 the Inspector General Act of 1978, the **[**annual**]** evalua-

tion 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) AGENCY REPORTING.—

(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.

(2) * * *

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

(f) PROTECTION OF INFORMATION.—

(1) Agencies, evaluators, and other recipients of information that, if disclosed, may cause grave harm to the efforts of Federal information security officers, including the appropriate congressional committees, shall take appropriate steps to ensure the protection of that information, including safeguarding the information from public disclosure.

(2) The protections required under paragraph (1) shall be commensurate with the risk and comply with all applicable laws and regulations.

(3) With respect to information that is not related to national security systems, agencies and evaluators shall make a summary of the information unclassified and publicly available, including information that does not identify—

(A) specific information system incidents; or

(B) specific information system vulnerabilities.

(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**[**.**]***;*

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

* * * * * * *

(i) * * *

[(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 guidance for evaluating the effectiveness of an information security program and practices

(2) PRIORITIES.—The guidance developed under paragraph (1) shall prioritize the identification of—

(A) the most common threat patterns experienced by each agency;

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

(C) any other security risks unique to the networks of each agency.

* * * * * * *

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) DEFINITIONS.—In this section:

(1) AGENCY OPERATIONAL PLAN.—The term 'agency operational plan' means a plan of an agency for the use of penetration testing.

(2) RULES OF ENGAGEMENT.—The term 'rules of engagement' means a set of rules established by an agency for the use of penetration testing.

(b) GUIDANCE.—

(1) IN GENERAL.—The Director shall issue guidance that—

(A) requires agencies to use, when and where appropriate, penetration testing on agency systems; and

(B) requires agencies to develop an agency operational plan and rules of engagement that meet the requirements under subsection (c).

(2) PENETRATION TESTING GUIDANCE.—The guidance issued under this section shall—

(A) permit an agency to use, for the purpose of performing penetration testing—

(i) a shared service of the agency or another agency; or

(ii) an external entity, such as a vendor; and

(B) require agencies to provide the rules of engagement and results of penetration testing to the Director and the Director of the Cybersecurity and Infrastructure Security

Agency, without regard to the status of the entity that performs the penetration testing.

(c) AGENCY PLANS AND RULES OF ENGAGEMENT.—The agency operational plan and rules of engagement of an agency shall—

(1) require the agency to—

(A) perform penetration testing on the high value assets of the agency; or

(B) coordinate with the Director of the Cybersecurity and Infrastructure Security Agency to ensure that penetration testing is being performed;

(2) establish guidelines for avoiding, as a result of penetration testing—

(A) adverse impacts to the operations of the agency;

(B) adverse impacts to operational environments and systems of the agency; and

(C) inappropriate access to data;

(3) require the results of penetration testing to include feedback to improve the cybersecurity of the agency; and

(4) include mechanisms for providing consistently formatted, and, if applicable, automated and machine-readable, data to the Director and the Director of the Cybersecurity and Infrastructure Security Agency.

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

(1) establish a process to assess the performance of penetration testing by both Federal and non-Federal entities that establishes minimum quality controls for penetration testing;

(2) develop operational guidance for instituting penetration testing programs at agencies;

(3) develop and maintain a centralized capability to offer penetration testing as a service to Federal and non-Federal entities; and

(4) provide guidance to agencies on the best use of penetration testing resources.

(e) RESPONSIBILITIES OF OMB.—The Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall—

(1) not less frequently than annually, inventory all Federal penetration testing assets; and

(2) develop and maintain a standardized process for the use of penetration testing.

(f) PRIORITIZATION OF PENETRATION TESTING RESOURCES.—

(1) IN GENERAL.—The Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall develop a framework for prioritizing Federal penetration testing resources among agencies.

(2) CONSIDERATIONS.—In developing the framework under this subsection, the Director shall consider—

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

(B) the Federal risk assessment performed under section 3553(i);

(C) the analysis of Federal incident data performed under section 3597; and

(D) any other information determined appropriate by the Director or the Director of the Cybersecurity and Infrastructure Security Agency.

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

(h) DELEGATION OF AUTHORITY FOR CERTAIN SYSTEMS.—The authorities of the Director described in subsection (b) 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 3553(e)(3).

SEC. 3559B. FEDERAL VULNERABILITY DISCLOSURE PROGRAMS

(a) DEFINITIONS.—In this section:

(1) REPORT.—The term 'report' means a vulnerability disclosure made to an agency by a reporter.

(2) REPORTER.—The term 'reporter' means an individual that submits a vulnerability report pursuant to the vulnerability disclosure process of an agency.

(b) Responsibilities of OMB.—

(1) LIMITATION ON LEGAL ACTION.—The Director, in consultation with the Attorney General, shall issue guidance to agencies to not recommend or pursue legal action against a reporter or an individual that conducts a security research activity that the head of the agency determines—

(A) represents a good faith effort to follow the vulnerability disclosure policy of the agency developed under subsection (d)(2); and

(B) is authorized under the vulnerability disclosure policy of the agency developed under subsection (d)(2).

(2) SHARING INFORMATION WITH CISA.—The Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director, shall issue guidance to agencies on sharing relevant information in a consistent, automated, and machine readable manner with the Cybersecurity and Infrastructure Security Agency, including—

(A) any valid or credible reports of newly discovered or not publicly known vulnerabilities (including misconfigurations) on Federal information systems that use commercial software or services;

(B) information relating to vulnerability disclosure, coordination, or remediation activities of an agency, particularly as those activities relate to outside organizations—

(i) with which the head of the agency believes the Director of the Cybersecurity and Infrastructure Security Agency can assist; or

(ii) about which the head of the agency believes the Director of the Cybersecurity and Infrastructure Security Agency should know; and

(C) any other information with respect to which the head of the agency determines helpful or necessary to involve the Cybersecurity and Infrastructure Security Agency.

(3) AGENCY VULNERABILITY DISCLOSURE POLICIES.—The Director shall issue guidance to agencies on the required minimum scope of agency systems covered by the vulnerability disclosure policy of an agency required under subsection (d)(2).

(c) 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; and

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

(d) 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—

(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;

(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; and

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

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

(i) how the reporter should submit the 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, to cover all Federal information systems used or operated by that agency or on behalf of that agency.

(3) IDENTIFIED VULNERABILITIES.—The head of each agency shall incorporate any vulnerabilities reported under paragraph (2) into the vulnerability management process of the agency in order to track and remediate the vulnerability.

(e) PAPERWORK REDUCTION ACT EXEMPTION.—The requirements of subchapter I (commonly known as the 'Paperwork Reduction Act') shall not apply to a vulnerability disclosure program established under this section.

(f) CONGRESSIONAL REPORTING.—Not later than 90 days after the date of enactment of the Federal Information Security Modernization Act of 2021, and annually thereafter for a 3-year period, the Director shall provide to the Committee on Homeland Security and

Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives a briefing on the status of the use of vulnerability disclosure policies under this section at agencies, including, with respect to the guidance issued under subsection (b)(3), an identification of the agencies that are compliant and not compliant.

(g) EXEMPTIONS.—The authorities and functions of the Director and Director of the Cybersecurity and Infrastructure Security Agency under 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).

* * * * * * *

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 Oversight and Reform of the House of Representatives;

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

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

(G) the Director;

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

(I) the National Cyber Director;

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

(K) the inspector general of any impacted agency.

(2) AWARDEE.—The term 'awardee'—

(A) means a person, business, or other entity that receives a grant from, or is a party to a cooperative agreement with, an agency; and

(B) includes any subgrantee of a person, business, or other entity described in subparagraph (A).

(3) BREACH.—The term 'breach' means—

(A) a compromise of the security, confidentiality, or integrity of data in electronic form that results in unauthorized access to, or an acquisition of, personal information; or

(B) a loss of data in electronic form that results in unauthorized access to, or an acquisition of, personal information.

(4) CONTRACTOR.—The term 'contractor' means—

(A) a prime contractor of an agency or a subcontractor of a prime contractor of an agency; and

(B) any person or business that collects or maintains information, including personally identifiable 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 used or operated by an agency, a contractor, or another organization on behalf of an agency.

(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.

SEC. 3592. NOTIFICATION OF BREACH

(a) 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 a senior privacy officer of the agency, shall—

(1) determine whether notice to any individual potentially affected by the breach is appropriate based on 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) as appropriate, provide written notice in accordance with subsection (b) 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 that the head of the agency or a designated senior-level individual of the agency selects based on factors determined by the Director.

(b) CONTENTS OF NOTICE.—Each notice of a breach provided to an individual under subsection (a)(2) shall include—

(1) a brief description of the rationale for the determination that notice should be provided under subsection (a);

(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 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 information to contact 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.

(c) DELAY OF NOTIFICATION.—

(1) IN GENERAL.—The Attorney General, the Director of National Intelligence, or the Secretary of Homeland Security may delay a notification required under subsection (a) if the notification would—

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

(B) reveal sensitive sources and methods;

(C) cause damage to national security; or

(D) hamper security remediation actions.

(2) DOCUMENTATION.—

(A) IN GENERAL.—Any delay under paragraph (1) shall be reported in writing to the Director, the Attorney General, the Director of National Intelligence, the Secretary of Homeland Security, the Director of the Cybersecurity and Infrastructure Security Agency, and the head of the agency and the inspector general of the agency that experienced the breach.

(B) CONTENTS.—A report required under subparagraph (A) shall include a written statement from the entity that delayed the notification explaining the need for the delay.

(C) FORM.—The report required under subparagraph (A) shall be unclassified but may include a classified annex.

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

(d) 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 (a)(1), or that it is necessary to update the details of the information provided to impacted individuals as described in subsection (b), 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 (a) of those changes.

(e) EXEMPTION FROM NOTIFICATION.—

(1) IN GENERAL.—The head of an agency, in consultation with the inspector general of the agency, may request an exemption from the Director from complying with the notification requirements under subsection (a) if the information affected by the breach is determined by an independent evaluation to be

unreadable, including, as appropriate, instances in which the information is—

(A) encrypted; and

(B) determined by the Director of the Cybersecurity and Infrastructure Security Agency to be of sufficiently low risk of exposure.

(2) APPROVAL.—The Director shall determine whether to grant an exemption requested under paragraph (1) in consultation with—

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

(B) the Attorney General.

(3) DOCUMENTATION.—Any exemption granted by the Director under paragraph (1) shall be reported in writing to the head of the agency and the inspector general of the agency that experienced the breach and the Director of the Cybersecurity and Infrastructure Security Agency.

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

(1) the Director from issuing guidance relating to notifications or the head of an agency from notifying individuals potentially affected by breaches that are not determined to be major incidents; or

(2) the Director from issuing guidance relating to notifications of major incidents or the head of an agency from providing more information than described in subsection (b) when notifying individuals potentially affected by breaches.

SEC. 3593. CONGRESSIONAL AND EXECUTIVE BRANCH REPORTS

(a) INITIAL REPORT.—

(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 report and, to the extent practicable, provide a briefing to the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, and the appropriate authorization and appropriations committees of Congress, taking into account—

(A) the information known at the time of the report;

(B) the sensitivity of the details associated with the major incident; and

(C) the classification level of the information contained in the report.

(2) CONTENTS.—A report required under paragraph (1) shall include, in a manner that excludes or otherwise reasonably protects personally identifiable information and to the extent permitted by applicable law, including privacy and statistical laws—

(A) a summary of the information available about the major incident, including how the major incident occurred, information indicating that the major incident may be a breach, and information relating to the major incident as

a breach, based on information available to agency officials as of the date on which the agency submits the report;

(B) if applicable, a description and any associated documentation of any circumstances necessitating a delay in or exemption to notification to individuals potentially affected by the major incident under subsection (c) or (e) of section 3592; and

(C) if applicable, an assessment of the impacts to the agency, the Federal Government, or the security of the United States, based on information available to agency officials on the date on which the agency submits the report.

(b) SUPPLEMENTAL REPORT.—Within a reasonable amount of time, but not later than 30 days after the date on which an agency submits a written report under subsection (a), the head of the agency shall provide to the appropriate reporting entities written updates on the major incident and, to the extent practicable, provide a briefing to the congressional committees described in subsection (a)(1), including summaries of—

(1) vulnerabilities, means by which the major incident occurred, and impacts to the agency relating to the major incident;

(2) any risk assessment and subsequent risk-based security implementation of the affected information system before the date on which the major incident occurred;

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

(4) an estimate of the number of individuals potentially affected by the major incident based on information available to agency officials as of the date on which the agency provides the update;

(5) an assessment of the risk of harm to individuals potentially affected by the major incident based on information available to agency officials as of the date on which the agency provides the update;

(6) 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 based on information available to agency officials as of the date on which the agency provides the update; and

(7) the detection, response, and remediation actions of the agency, including any support provided by the Cybersecurity and Infrastructure Security Agency under section 3594(d) and status updates on the notification process described in section 3592(a), including any delay or exemption described in subsection (c) or (e), respectively, of section 3592, if applicable.

(c) UPDATE REPORT.—If the agency determines that there is any significant change in the understanding of the agency of the scope, scale, or consequence of a major incident for which an agency submitted a written report under subsection (a), the agency shall provide an updated report to the appropriate reporting entities that includes information relating to the change in understanding.

(d) ANNUAL REPORT.—Each agency shall submit as part of the annual report required under section 3554(c)(1) of this title a de-

scription of each major incident that occurred during the 1-year period preceding the date on which the report is submitted.

(e) DELAY AND EXEMPTION REPORT.—

(1) IN GENERAL.—The Director shall submit to the appropriate notification entities an annual report on all notification delays and exemptions granted pursuant to subsections (c) and (d) of section 3592.

(2) COMPONENT OF OTHER REPORT.—The Director may submit the report required under paragraph (1) as a component of the annual report submitted under section 3597(b).

(f) REPORT DELIVERY.—Any written report required to be submitted under this section may be submitted in a paper or electronic format.

(g) THREAT BRIEFING.—

(1) IN GENERAL.—Not later than 7 days after the date on which an agency has a reasonable basis to conclude that a major incident occurred, the head of the agency, jointly with the National Cyber Director and any other Federal entity determined appropriate by the National Cyber Director, shall provide a briefing to the congressional committees described in subsection (a)(1) on the threat causing the major incident.

(2) COMPONENTS.—The briefing required under paragraph (1)—

(A) shall, to the greatest extent practicable, include an unclassified component; and

(B) may include a classified component.

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

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

(2) Congress from requesting additional information from agencies through reports, briefings, or other means.

SEC. 3594. GOVERNMENT INFORMATION SHARING AND INCIDENT RESPONSE

(a) IN GENERAL.—

(1) INCIDENT REPORTING.—The head of each agency shall provide any information relating to any incident, whether the information is obtained by the Federal Government directly or indirectly, to the Cybersecurity and Infrastructure Security Agency and the Office of Management and Budget.

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

(A) include detailed information about the safeguards that were in place when the incident occurred;

(B) whether the agency implemented the safeguards described in subparagraph (A) correctly;

(C) in order to protect against a similar incident, identify—

(i) how the safeguards described in subparagraph (A) should be implemented differently; and

(ii) additional necessary safeguards; and

(D) include 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 the party that conducted the incident.

(3) INFORMATION SHARING.—To the greatest extent practicable, the Director of the Cybersecurity and Infrastructure Security Agency shall share information relating to an incident with any agencies that may be impacted by the incident.

(4) NATIONAL SECURITY SYSTEMS.—Each agency operating or exercising control of a national security system shall share information about incidents with 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) COMPLIANCE.—The information provided under subsection (a) shall take into account the level of classification of the information and any information sharing limitations and protections, such as limitations and protections relating to law enforcement, national security, privacy, statistical confidentiality, or other factors determined by the Director

(c) INCIDENT RESPONSE.—Each agency that has a reasonable basis to conclude that a major incident occurred involving Federal information in electronic medium or form, as defined by the Director and not involving a national security system, regardless of delays from notification granted for a major incident, shall coordinate with the Cybersecurity and Infrastructure Security Agency regarding—

(1) incident response and recovery; and

(2) recommendations for mitigating future incidents.

SEC. 3595. RESPONSIBILITIES OF CONTRACTORS AND AWARDEES.“3595. RESPONSIBILITIES OF CONTRACTORS AND AWARDEES

(a) NOTIFICATION.—

(1) IN GENERAL.—Unless otherwise specified in a contract, grant, or cooperative agreement, any contractor or awardee of an agency shall report to the agency within the same amount of time such agency is required to report an incident to the Cybersecurity and Infrastructure Security 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 collected, used, or maintained by the contractor or awardee in connection with the contract, grant, or cooperative agreement of the contractor or awardee;

(B) an incident or breach has occurred with respect to a Federal information system used or operated by the contractor or awardee in connection with the contract, grant, or cooperative agreement of the contractor or awardee; or

(C) the contractor or awardee has received information from the agency that the contractor or awardee is not authorized to receive in connection with the contract, grant, or cooperative agreement of the contractor or awardee.

(2) PROCEDURES.—

(A) MAJOR INCIDENT.—Following a report of a breach or major incident by a contractor or awardee under para-

graph (1), the agency, in consultation with the contractor or awardee, shall carry out the requirements under sections 3592, 3593, and 3594 with respect to the major incident.

(B) INCIDENT.—Following a report of an incident by a contractor or awardee under paragraph (1), an agency, in consultation with the contractor or awardee, shall carry out the requirements under section 3594 with respect to the incident.

(b) EFFECTIVE DATE.—This section shall apply on and after the date that is 1 year after the date of enactment of the Federal Information Security Modernization Act of 2021.

SEC. 3596. TRAINING

(a) COVERED INDIVIDUAL DEFINED.—In this section, the term 'covered individual' means an individual who obtains access to Federal information or Federal information systems because of the status of the individual as an employee, contractor, awardee, volunteer, or intern of an agency.

(b) REQUIREMENT.—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 a confirmed major incident and any suspected incident involving information in any medium or form, including paper, oral, and electronic.

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

SEC. 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 develop, in consultation with the Director and the National Cyber Director, and perform 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) cross Federal Government root causes of incidents at agencies;

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

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

(2) AUTOMATED ANALYSIS.—The analyses developed under paragraph (1) shall, to the greatest extent practicable, use ma-

chine readable data, automation, and machine learning processes.

(3) SHARING OF DATA AND ANALYSIS.—

(A) IN GENERAL.—The Director shall share on an ongoing basis the analyses required under this subsection with agencies 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 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.

(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 and other Federal agencies as appropriate, shall submit to the appropriate notification 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), including specific analysis of breaches, on an agency-by-agency basis and comprehensively across the Federal Government; and

(3) an annex for each agency that includes—

(A) a description of each major incident; and

(B) the total number of compromises of the agency.

(c) PUBLICATION.—A version of each report submitted under subsection (b) shall be made publicly available on the website of the Cybersecurity and Infrastructure Security Agency during the year in which the report is submitted.

(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.—

(A) IN GENERAL.—Subject to subparagraph (B), 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—

(i) data for the incident; and

(ii) the information described in subsection (b) with respect to the agency.

(B) EXCEPTION FOR NATIONAL SECURITY SYSTEMS.—The head of an agency that owns or exercises control of a national security system shall not include data for an incident

that occurs on a national security system in any report submitted under subparagraph (A).

(3) NATIONAL SECURITY SYSTEM REPORTS.—

(A) IN GENERAL.—Annually, the head of an agency that operates or exercises control of a national security system shall submit a report that includes the information described in subsection (b) with respect to the agency 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—

(i) the the majority and minority leaders of the Senate,

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

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

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

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

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

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

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

(ix) the Committee on Armed Services of the House of Representatives.

(B) CLASSIFIED FORM.—A report required under subparagraph (A) may be submitted in a classified form.

(e) REQUIREMENT FOR COMPILING INFORMATION.—In publishing the public report required under subsection (c), the Director of the Cybersecurity and Infrastructure Security Agency shall sufficiently compile information such that no specific incident of an agency can be identified, except with the concurrence of the Director of the Office of Management and Budget and in consultation with the impacted agency.

SEC. 3598. MAJOR INCIDENT DEFINITION

(a) IN GENERAL.—Not later than 180 days after the date of enactment of the Federal Information Security Modernization Act of 2021, the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director, shall develop 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 an information system used or operated by an agency or by a contractor of an agency or another organization on behalf of an agency—

(A) any incident the head of the agency determines is likely to have an impact on—

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

(ii) the civil liberties 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 for the agency, a component of the agency, or the Federal Government, to provide 1 or more critical services;

(C) any incident that the head of an agency, in consultation with a senior privacy officer of the agency, determines is likely to have a significant privacy impact on 1 or more individual;

(D) any incident that the head of the agency, in consultation with a senior privacy official of the agency, determines is likely to have a substantial privacy impact on a significant number of individuals;

(E) any incident the head of the agency determines impacts the operations of a high value asset owned or operated by the agency;

(F) any incident involving the exposure of sensitive agency information to a foreign entity, 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

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

(2) stipulate that the National Cyber Director shall declare a major incident at each agency impacted by an incident if the Director of the Cybersecurity and Infrastructure Security Agency determines 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, a common software or hardware vulnerability; or

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

(3) stipulate that, in determining whether an incident constitutes a major incident because that incident—

(A) is any incident described in paragraph (1), the head of an agency shall consult with the Director of the Cybersecurity and Infrastructure Security Agency;

(B) is an incident described in paragraph (1)(A), the head of the agency shall consult with the National Cyber Director; and

(C) is an incident described in subparagraph (C) or (D) of paragraph (1), the head of the agency shall consult with—

(i) the Privacy and Civil Liberties Oversight Board; and

(ii) the Executive Director of the Federal Trade Commission.

(c) SIGNIFICANT NUMBER OF INDIVIDUALS.—In determining what constitutes a significant number of individuals under subsection (b)(1)(D), the Director—

(1) may determine a threshold for a minimum number of individuals that constitutes a significant amount; and

(2) may not determine a threshold described in paragraph (1) that exceeds 5,000 individuals.

(d) EVALUATION AND UPDATES.—Not later than 2 years after the date of enactment of the Federal Information Security Modernization Act of 2021, and not less frequently than every 2 years thereafter, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives an evaluation, which shall include—

(1) an update, if necessary, to the guidance issued under subsection (a);

(2) the definition of the term 'major incident' included in the guidance issued under subsection (a); and

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

* * * * * * *

HOMELAND SECURITY ACT OF 2002

* * * * * * *

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.

* * * * * * *

CYBERSECURITY ACT OF 2015

* * * * * * *

TITLE II—NATIONAL CYBERSECURITY ADVANCEMENT

* * * * * * *

Subtitle B—Federal Cybersecurity Enhancement

* * * * * * *

SEC. 226. ASSESSMENT; REPORTS.

(a) * * *

(b) * * *

(c) REPORTS TO CONGRESS

(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 under section 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 under section 3553(c) of title 44] *that report*.

* * * * * * *

○