Calendar No. 265

117TH CONGRESS
2D SESSION

S. 3600

To improve the cybersecurity of the Federal Government, and for other purposes.

IN THE SENATE OF THE UNITED STATES

FEBRUARY 8 (legislative day, FEBRUARY 3), 2022

Mr. PETERS (for himself and Mr. PORTMAN) introduced the following bill; which was read the first time

FEBRUARY 9, 2022

Read the second time and placed on the calendar

A BILL

To improve the cybersecurity of the Federal Government, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Strengthening American Cybersecurity Act of 2022''.

SEC. 2. TABLE OF CONTENTS.

The table of contents for this Act is as follows:

TITLE I—FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2022

SEC. 101. SHORT TITLE.

This title may be cited as the ''Federal Information Security Modernization Act of 2022''.

SEC. 102. DEFINITIONS.

In this title, unless otherwise specified:

(1) ADDITIONAL CYBERSECURITY PROCEDURE.—The term ''additional cybersecurity procedure'' has the meaning given the term in section 3552(b) of title 44, United States Code, as amended by this title.

(2) AGENCY.—The term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code.

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

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

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

(C) the Committee on Homeland Security of the House of Representatives.

(4) DIRECTOR.—The term ''Director'' means the Director of the Office of Management and Budget.

(5) INCIDENT.—The term ''incident'' has the meaning given the term in section 3552(b) of title 44, United States Code.

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

(7) PENETRATION TEST.—The term ''penetration test'' has the meaning given the term in section 3552(b) of title 44, United States Code, as amended by this title.

(8) THREAT HUNTING.—The term ''threat hunting'' means proactively and iteratively searching systems for threats that evade detection by automated threat detection systems.

SEC. 103. TITLE 44 AMENDMENTS.

(a) SUBCHAPTER I AMENDMENTS.—Subchapter I of chapter 35 of title 44, United States Code, is amended—

(1) in section 3504—

(A) in subsection (a)(1)(B)—

(i) by striking clause (v) and inserting the following:

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

(ii) by redesignating clause (vi) as clause (vii); and

(iii) by inserting after clause (v) the following:

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

(B) in subsection (g), by striking paragraph (1) and inserting the following:

''(1) develop and oversee the implementation of policies, principles, standards, and guidelines on privacy, confidentiality, disclosure, and sharing, and in consultation with the National Cyber Director, oversee the implementation of policies, principles, standards, and guidelines on security, of information collected or maintained by or for agencies; and'';

(2) in section 3505—

(A) by striking the first subsection designated as subsection (c);

(B) in paragraph (2) of the second subsection designated as subsection (c), by inserting ''an identification of internet accessible in-

formation systems and'' after ''an inventory under this subsection shall include'';

(C) in paragraph (3) of the second subsection designated as subsection (c)—

(i) in subparagraph (B)—

(I) by inserting ''the Director of the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, and'' before ''the Comptroller General''; and

(II) by striking ''and'' at the end;

(ii) in subparagraph (C)(v), by striking the period at the end and inserting ''; and''; and

(iii) by adding at the end the following:

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

(3) in section 3506—

(A) in subsection (a)(3), by inserting ''In carrying out these duties, the Chief Information Officer shall coordinate, as appropriate, with the Chief Data Officer in accordance with the designated functions under section 3520(c).''

after ''reduction of information collection burdens on the public.'';

(B) in subsection (b)(1)(C), by inserting '', availability'' after ''integrity''; and

(C) in subsection (h)(3), by inserting ''security,'' after ''efficiency,''; and

(4) in section 3513—

(A) by redesignating subsection (c) as subsection (d); and

(B) by inserting after subsection (b) the following:

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

(b) SUBCHAPTER II DEFINITIONS.—

(1) IN GENERAL.—Section 3552(b) of title 44, United States Code, is amended—

(A) by redesignating paragraphs (1), (2), (3), (4), (5), (6), and (7) as paragraphs (2), (4), (5), (6), (7), (9), and (11), respectively;

(B) by inserting before paragraph (2), as so redesignated, the following:

''(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.'';

(C) by inserting after paragraph (2), as so redesignated, the following:

''(3) The term 'high value asset' means information or an information system that the head of an agency, using policies, principles, standards, or guidelines issued by the Director under section 3553(a), determines to be so critical to the agency that the loss or 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.'';

(D) by inserting after paragraph (7), as so redesignated, the following:

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

(E) by inserting after paragraph (9), as so redesignated, the following:

''(10) The term 'penetration test'—

''(A) means an authorized assessment that emulates attempts to gain unauthorized access to, or disrupt the operations of, an information system or component of an information system; and

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

(F) by inserting after paragraph (11), as so redesignated, the following:

''(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.''.

(2) CONFORMING AMENDMENTS.—

(A) HOMELAND SECURITY ACT OF 2002.—Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(1)(A)) is amended by striking ''section 3552(b)(5)'' and inserting ''section 3552(b)''.

(B) TITLE 10.—

(i) SECTION 2222.—Section 2222(i)(8) of title 10, United States Code, is amended

by striking ''section 3552(b)(6)(A)'' and inserting ''section 3552(b)(9)(A)''.

(ii) SECTION 2223.—Section 2223(c)(3) of title 10, United States Code, is amended by striking ''section 3552(b)(6)'' and inserting ''section 3552(b)''.

(iii) SECTION 2315.—Section 2315 of title 10, United States Code, is amended by striking ''section 3552(b)(6)'' and inserting ''section 3552(b)''.

(iv) SECTION 2339A.—Section 2339a(e)(5) of title 10, United States Code, is amended by striking ''section 3552(b)(6)'' and inserting ''section 3552(b)''.

(C) HIGH-PERFORMANCE COMPUTING ACT OF 1991.—Section 207(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5527(a)) is amended by striking ''section 3552(b)(6)(A)(i)'' and inserting ''section 3552(b)(9)(A)(i)''.

(D) INTERNET OF THINGS CYBERSECURITY IMPROVEMENT ACT OF 2020.—Section 3(5) of the Internet of Things Cybersecurity Im-

provement Act of 2020 (15 U.S.C. 278g–3a) is amended by striking ''section 3552(b)(6)'' and inserting ''section 3552(b)''.

(E) NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2013.—Section 933(e)(1)(B) of the National Defense Authorization Act for Fiscal Year 2013 (10 U.S.C. 2224 note) is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552(b)''.

(F) IKE SKELTON NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011.—The Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111–383) is amended—

(i) in section 806(e)(5) (10 U.S.C. 2304 note), by striking ''section 3542(b)'' and inserting ''section 3552(b)'';

(ii) in section 931(b)(3) (10 U.S.C. 2223 note), by striking ''section 3542(b)(2)'' and inserting ''section 3552(b)''; and

(iii) in section 932(b)(2) (10 U.S.C. 2224 note), by striking ''section 3542(b)(2)'' and inserting ''section 3552(b)''.

(G) E-GOVERNMENT ACT OF 2002.—Section 301(c)(1)(A) of the E-Government Act of 2002 (44 U.S.C. 3501 note) is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552(b)''.

(H) NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ACT.—Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended—

(i) in subsection (a)(2), by striking ''section 3552(b)(5)'' and inserting ''section 3552(b)''; and

(ii) in subsection (f)—

(I) in paragraph (3), by striking ''section 3532(1)'' and inserting ''section 3552(b)''; and

(II) in paragraph (5), by striking ''section 3532(b)(2)'' and inserting ''section 3552(b)''.

(c) SUBCHAPTER II AMENDMENTS.—Subchapter II of chapter 35 of title 44, United States Code, is amended—

(1) in section 3551—

(A) in paragraph (4), by striking ''diagnose and improve'' and inserting ''integrate, deliver, diagnose, and improve'';

(B) in paragraph (5), by striking ''and'' at the end;

(C) in paragraph (6), by striking the period at the end and inserting a semi colon; and

(D) by adding at the end the following:

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

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

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

(2) in section 3553—

(A) in subsection (a)—

(i) in paragraph (1), by inserting '', in consultation with the Secretary and the

National Cyber Director,'' before ''overseeing'';

(ii) in paragraph (5), by striking ''and'' at the end; and

(iii) by adding at the end the following:

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

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

''(B) the use of presumption of compromise and least privilege principles to improve resiliency and timely response actions to incidents on Federal systems.'';

(B) in subsection (b)—

(i) in the matter preceding paragraph (1), by inserting ''and the National Cyber Director'' after ''Director''; and

(ii) in paragraph (2)(A), by inserting ''and reporting requirements under sub-

chapter IV of this chapter'' after ''section 3556''; and

(C) in subsection (c)—

(i) in the matter preceding paragraph (1)—

(I) by striking ''each year'' and inserting ''each year during which agencies are required to submit reports under section 3554(c)''; and

(II) by striking ''preceding year'' and inserting ''preceding 2 years'';

(ii) by striking paragraph (1);

(iii) by redesignating paragraphs (2), (3), and (4) as paragraphs (1), (2), and (3), respectively;

(iv) in paragraph (3), as so redesignated, by striking ''and'' at the end;

(v) by inserting after paragraph (3), as so redesignated the following:

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

(vi) in paragraph (5), by striking the period at the end and inserting ''; and'';

(D) by redesignating subsections (i), (j), (k), and (l) as subsections (j), (k), (l), and (m) respectively;

(E) by inserting after subsection (h) the following:

''(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 cyber 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.'';

(F) in subsection (j), as so redesignated—

(i) by striking ''regarding the specific'' and inserting ''that includes a summary of—

''(1) the specific'';

(ii) in paragraph (1), as so designated, by striking the period at the end and inserting ''; and'' and

(iii) by adding at the end the following:

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

(G) by adding at the end the following:

''(n) BINDING OPERATIONAL DIRECTIVES.—If the Director of the Cybersecurity and Infrastructure Security Agency issues a binding operational directive or an emer-

gency directive under this section, not later than 4 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 Director, National Cyber Director, the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives the status of the implementation of the binding operational directive at the agency.'';

(3) in section 3554—

(A) in subsection (a)—

(i) in paragraph (1)—

(I) by redesignating subparagraphs (A), (B), and (C) as subparagraphs (B), (C), and (D), respectively;

(II) by inserting before subparagraph (B), as so redesignated, the following:

''(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 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;

"(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;'';

(III) in subparagraph (B), as so redesignated, in the matter preceding clause (i), by striking ''providing information'' and inserting ''using information from the assessment con-

ducted under subparagraph (A), providing information'';

(IV) in subparagraph (C), as so redesignated—

(aa) in clause (ii) by inserting ''binding'' before ''operational''; and

(bb) in clause (vi), by striking ''and'' at the end; and

(V) by adding at the end the following:

''(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;'';

(ii) in paragraph (2)—

(I) in subparagraph (A), by inserting ''in accordance with the agency system risk assessment performed under paragraph (1)(A)'' after ''information systems'';

(II) in subparagraph (B)—

(aa) by striking ''in accordance with standards'' and inserting ''in accordance with—

''(i) standards''; and

(bb) by adding at the end the following:

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

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

(III) in subparagraph (D), by inserting '', through the use of penetration testing, the vulnerability disclo-

sure program established under section 3559B, and other means,'' after ''periodically'';

(iii) in paragraph (3)—

(I) in subparagraph (A)—

(aa) in clause (iii), by striking ''and'' at the end;

(bb) in clause (iv), by adding ''and'' at the end; and

(cc) by adding at the end the following:

''(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;''; and

(iv) in paragraph (5), by inserting ''and the Director of the Cybersecurity and Infrastructure Security Agency'' before ''on the effectiveness'';

(B) in subsection (b)—

(i) by striking paragraph (1) and inserting the following:

''(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;'';

(ii) in paragraph (2)—

(I) by striking subparagraph (B) and inserting the following:

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

(II) in subparagraph (D)—

(aa) by redesignating clauses (iii) and (iv) as clauses (iv) and (v), respectively;

(bb) by inserting after clause (ii) the following:

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

(cc) in clause (iv), as so redesignated, by striking ''as determined by the agency; and'' and inserting ''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'';

(iii) in paragraph (5)(A), by inserting ", including penetration testing, as appropriate," after "shall include testing";

(iv) in paragraph (6), by striking "planning, implementing, evaluating, and documenting" and inserting "planning and implementing and, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, evaluating and documenting";

(v) by redesignating paragraphs (7) and (8) as paragraphs (8) and (9), respectively;

(vi) by inserting after paragraph (6) the following:

"(7) a process for providing the status of every remedial action and unremediated identified 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;"; and

(vii) in paragraph (8)(C), as so redesignated—

(I) by striking clause (ii) and inserting the following:

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

(II) by redesignating clause (iii) as clause (iv);

(III) by inserting after clause (ii) the following:

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

(IV) in clause (iv), as so redesignated—

(aa) in subclause (I), by striking ''and relevant offices of inspectors general'';

(bb) in subclause (II), by adding ''and'' at the end;

(cc) by striking subclause (III); and

(dd) by redesignating subclause (IV) as subclause (III);

(C) in subsection (c)—

(i) by redesignating paragraph (2) as paragraph (5);

(ii) by striking paragraph (1) and inserting the following:

"(1) BIANNUAL REPORT.—Not later than 2 years after the date of enactment of the Federal Information Security Modernization Act of 2022 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 majority and minority leaders of the Senate, the Speaker and minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, the Committee on Commerce, Science, and Transportation of the Senate, the Committee on Science, Space, and Technology of the House of Representatives, 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), including an analysis of the agency's cybersecurity and incident response capabilities using the metrics established under section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c));

"(C) summarizes the 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.''; and

(iii) in paragraph (5), as so redesignated, by striking the period at the end and inserting '', including the reporting procedures established under section 11315(d) of title 40 and subsection (a)(3)(A)(v) of this section''; and

(D) in subsection (d)(1), in the matter preceding subparagraph (A), by inserting ''and the

National Cyber Director'' after ''the Director''; and

(E) by adding at the end the following:

''(f) REPORTING STRUCTURE EXEMPTION.—

''(1) IN GENERAL.—On an annual basis, the Director may exempt an agency from the reporting structure requirement under subsection (a)(3)(A)(v)(II).

''(2) REPORT.—On an annual basis, the Director shall submit a report to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives that includes a list of each exemption granted under paragraph (1) and the associated rationale for each exemption.

''(3) COMPONENT OF OTHER REPORT.—The report required under paragraph (2) may be incorporated into any other annual report required under this chapter.'';

(4) in section 3555—

(A) in the section heading, by striking ''**ANNUAL INDEPENDENT**'' and inserting ''**INDEPENDENT**'';

(B) in subsection (a)—

(i) in paragraph (1), by inserting ''during which a report is required to be submitted under section 3553(c),'' after ''Each year'';

(ii) in paragraph (2)(A), by inserting '', including by penetration testing and analyzing the vulnerability disclosure program of the agency'' after ''information systems''; and

(iii) by adding at the end the following:

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

(C) in subsection (b)(1), by striking ''annual'';

(D) in subsection (e)(1), by inserting ''during which a report is required to be submitted under section 3553(c)'' after ''Each year'';

(E) by striking subsection (f) and inserting the following:

''(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, 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.'';

(F) in subsection (g)(2)—

(i) by striking ''this subsection shall'' and inserting ''this subsection—

''(A) shall'';

(ii) in subparagraph (A), as so designated, by striking the period at the end and inserting ''; and''; and

(iii) by adding at the end the following:

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

(G) by striking subsection (j) and inserting the following:

''(j) GUIDANCE.—

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

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

''(A) the identification of the most common successful threat patterns experienced by each agency;

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

''(C) any other security risks unique to the networks of each agency; and

''(D) any other element the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the

Council of the Inspectors General on Integrity and Efficiency, determines appropriate.''; and

(5) in section 3556(a)—

(A) in the matter preceding paragraph (1), by inserting ''within the Cybersecurity and Infrastructure Security Agency'' after ''incident center''; and

(B) in paragraph (4), by striking ''3554(b)'' and inserting ''3554(a)(1)(A)''.

(d) CONFORMING AMENDMENTS.—

(1) TABLE OF SECTIONS.—The table of sections for chapter 35 of title 44, United States Code, is amended by striking the item relating to section 3555 and inserting the following:

''3555. Independent evaluation''.

(2) OMB REPORTS.—Section 226(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1524(c)) is amended—

(A) in paragraph (1)(B), in the matter preceding clause (i), by striking ''annually thereafter'' and inserting ''thereafter during the years during which a report is required to be submitted under section 3553(c) of title 44, United States Code''; and

(B) in paragraph (2)(B), in the matter preceding clause (i)—

(i) by striking ''annually thereafter'' and inserting ''thereafter during the years during which a report is required to be submitted under section 3553(c) of title 44, United States Code''; and

(ii) by striking ''the report required under section 3553(c) of title 44, United States Code'' and inserting ''that report''.

(3) NIST RESPONSIBILITIES.—Section 20(d)(3)(B) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(d)(3)(B)) is amended by striking ''annual''.

(e) FEDERAL SYSTEM INCIDENT RESPONSE.—

(1) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by adding at the end the following:

''SUBCHAPTER IV—FEDERAL SYSTEM INCIDENT RESPONSE

''§ 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 or an other transaction 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'—

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

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

''(4) CONTRACTOR.—The term 'contractor' means a prime contractor of an agency or a subcontractor of a prime contractor 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 con-

tractor, an awardee, 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.

''§ 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 breach;

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

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

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

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

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

''(5) any applicable educational materials relating to what individuals can do in response to a breach that potentially affects their personally identifiable information, including relevant contact information for 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) or (d) 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 National Cyber Director, 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 potentially affected 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) 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.

"§ 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 a notification to individuals potentially affected by the major incident under section 3592(c);

"(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; and

"(D) if applicable, whether any ransom has been demanded or paid, or plans to be paid, by any entity operating a Federal information system or with access to a Federal information

system, unless disclosure of such information may disrupt an active Federal law enforcement or national security operation.

''(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, which may include classified annexes, on the major incident and, to the extent practicable, provide a briefing, which may include a classified component, 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 that are directly related to the cause of the incident, 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;

''(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 described in section 3592(c), if applicable; and

''(8) if applicable, a description of any circumstances or data leading the head of the agency to determine, pursuant to section 3592(a)(1), not to notify individuals potentially impacted by a breach.

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

''(e) DELAY AND LACK OF NOTIFICATION REPORT.—

''(1) IN GENERAL.—The Director shall submit to the appropriate reporting entities an annual report on all notification delays granted pursuant to section 3592(c).

''(2) LACK OF BREACH NOTIFICATION.—The Director shall submit to the appropriate reporting entities an annual report on each breach with respect to which the head of an agency determined, pursuant to section 3592(a)(1), not to notify individuals potentially impacted by the breach.

''(3) 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 Director, 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.

''§ 3594. Government information sharing and incident response

''(a) IN GENERAL.—

''(1) INCIDENT REPORTING.—Subject to the limitations described in subsection (b), the head of each agency shall provide any information relating to any incident affecting the agency, whether the information is obtained by the Federal Government directly or indirectly, to the Cybersecurity and Infrastructure Security Agency.

''(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 or the cause of the incident, subject to appropriate privacy protections.

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

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

"(B) to the greatest extent practicable, share information relating to an incident with the head of any agency that may be—

"(i) impacted by the incident;

"(ii) similarly susceptible to the incident; or

"(iii) similarly targeted by the incident; and

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

"(4) NATIONAL SECURITY SYSTEMS.—Each agency operating or exercising control of a national security system shall share information about incidents that occur on national security systems 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.—In providing information and selecting a method to provide information under subsection (a), the head of each agency shall take into account the level of classification of the information and any information sharing limitations and protections, such as limita-

tions and protections relating to law enforcement, national security, privacy, statistical confidentiality, or other factors determined by the Director in order to implement subsection (a)(1) in a manner that enables automated and consistent reporting to the greatest extent practicable.

''(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 that does not exclusively involve a national security system, regardless of delays from notification granted for a major incident that is also a breach, shall coordinate with the Cybersecurity and Infrastructure Security Agency to facilitate asset response activities and provide recommendations for mitigating future incidents.

"§ 3595. Responsibilities of contractors and awardees

''(a) REPORTING.—

''(1) IN GENERAL.—Unless otherwise specified in a contract, grant, cooperative agreement, or an other transaction 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 suspect or 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, cooperative agreement, or other transaction 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, cooperative agreement, or other transaction 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, cooperative agreement, or other transaction 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 paragraph (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—

''(1) on and after the date that is 1 year after the date of enactment of the Federal Information Security Modernization Act of 2022; and

''(2) with respect to any contract entered into on or after the date described in paragraph (1).

''§ 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.

''§ 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) common root causes of incidents across multiple Federal agencies;

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

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

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

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

"(3) SHARING OF DATA AND ANALYSIS.—

"(A) IN GENERAL.—The Director 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, the National Cyber Director and the heads of other Federal agencies, as appropriate, shall submit to the appropriate reporting entities a report that includes—

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

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

''(A) a specific analysis of breaches; and

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

''(3) an annex for each agency that includes—

''(A) a description of each major incident;

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

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

''(c) PUBLICATION.—

''(1) IN GENERAL.—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.

''(2) EXEMPTION.—The Director of the Cybersecurity and Infrastructure Security Agency may exempt all or a portion of a report described in paragraph (1) from public publication if the Director of the Cybersecurity and Infrastructure Security Agency determines the exemption is in the interest of national security.

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

''(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 coordina-

tion with the Director of the Cybersecurity and Infrastructure Security Agency and the Director, shall submit to the appropriate reporting entities a report that includes the information described in subsection (b) with respect to the agency.

''(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 national security system 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 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 Appropriations of the Senate;

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

''(viii) the Committee on Homeland Security of the House of Representatives;

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

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

''(xi) the Committee on Appropriations 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.

"§ 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 2022, 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 substantially disrupts 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, in consultation with the Director, shall declare a major incident at each agency impacted by an incident if it is determined that an incident—

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

''(B) is enabled by—

''(i) a common technical root cause, such as a supply chain compromise, 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 is any incident described in paragraph (1),

the head of the agency shall consult with the National Cyber Director and may consult with the Director of the Cybersecurity and Infrastructure Security Agency.

''(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 2022, and not less frequently than every 2 years thereafter, the Director shall provide a briefing to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives, which shall include—

''(1) an evaluation of any necessary updates to the guidance issued under subsection (a);

''(2) an evaluation of any necessary updates to 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).''.

(2) CLERICAL AMENDMENT.—The table of sections for chapter 35 of title 44, United States Code, is amended by adding at the end the following:

''SUBCHAPTER IV—FEDERAL SYSTEM INCIDENT RESPONSE

SEC. 104. AMENDMENTS TO SUBTITLE III OF TITLE 40.

(a) MODERNIZING GOVERNMENT TECHNOLOGY.—Subtitle G of title X of Division A of the National Defense Authorization Act for Fiscal Year 2018 (40 U.S.C. 11301 note) is amended in section 1078—

(1) by striking subsection (a) and inserting the following:

''(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.'';

(2) in subsection (b), by adding at the end the following:

''(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 member of the Technology Modernization Board described in subsection (c)(5)(C).''; and

(3) in subsection (c)—

(A) in paragraph (2)(A)(i), by inserting '', including a consideration of the impact on high value assets'' after ''operational risks'';

(B) in paragraph (5)—

(i) in subparagraph (A), by striking ''and'' at the end;

(ii) in subparagraph (B), by striking the period at the end and inserting ''and''; and

(iii) by adding at the end the following:

''(C) a senior official from the Cybersecurity and Infrastructure Security Agency of the

Department of Homeland Security, appointed by the Director.''; and

(C) in paragraph (6)(A), by striking ''shall be—'' and all that follows through ''4 employees'' and inserting ''shall be 4 employees''.

(b) SUBCHAPTER I.—Subchapter I of chapter 113 of subtitle III of title 40, United States Code, is amended—

(1) in section 11302—

(A) in subsection (b), by striking ''use, security, and disposal of'' and inserting ''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,'';

(B) in subsection (c)—

(i) in paragraph (3)—

(I) in subparagraph (A)—

(aa) by striking ''including data'' and inserting ''which shall—

''(i) include data''; and

(bb) by adding at the end the following:

''(ii) specifically denote cybersecurity funding under the risk-based cyber budget

model developed pursuant to section 3553(a)(7) of title 44.''; and

(II) in subparagraph (B), by adding at the end the following:

''(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.'';

(C) in subsection (f)—

(i) by striking ''heads of executive agencies to develop'' and inserting ''heads of executive agencies to—

''(1) develop'';

(ii) in paragraph (1), as so designated, by striking the period at the end and inserting ''; and''; and

(iii) by adding at the end the following:

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

(D) in subsection (h), by inserting ", including cybersecurity performances," after "the performances"; and

(2) in section 11303(b)—

(A) in paragraph (2)(B)—

(i) in clause (i), by striking "or" at the end;

(ii) in clause (ii), by adding "or" at the end; and

(iii) by adding at the end the following:

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

(B) in paragraph (5)(B)(i), by inserting ", while taking into account the risk-based cyber budget model developed pursuant to section 3553(a)(7) of title 44" after "title 31".

(c) SUBCHAPTER II.—Subchapter II of chapter 113 of subtitle III of title 40, United States Code, is amended—

(1) in section 11312(a), by inserting ", including security risks" after "managing the risks";

(2) in section 11313(1), by striking ''efficiency and effectiveness'' and inserting ''efficiency, security, and effectiveness'';

(3) in section 11315, by adding at the end the following:

''(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.

''(e) REPORTING STRUCTURE EXEMPTION.—

''(1) IN GENERAL.—On annual basis, the Director may exempt any agency from the reporting structure requirements under subsection (d).

''(2) REPORT.—On an annual basis, 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 a report that includes a list of each exemption granted under paragraph (1) and the associated rationale for each exemption.

''(3) COMPONENT OF OTHER REPORT.—The report required under paragraph (2) may be incorporated into any other annual report required under chapter 35 of title 44, United States Code.'';

(4) in section 11317, by inserting ''security,'' before ''or schedule''; and

(5) in section 11319(b)(1), in the paragraph heading, by striking ''CIOS'' and inserting ''CHIEF INFORMATION OFFICERS''.

(d) SUBCHAPTER III.—Section 11331 of title 40, United States Code, is amended—

(1) in subsection (a), by striking ''section 3532(b)(1)'' and inserting ''section 3552(b)'';

(2) in subsection (b)(1)(A), by striking ''the Secretary of Homeland Security'' and inserting ''the Director of the Cybersecurity and Infrastructure Security Agency'';

(3) by striking subsection (c) and inserting the following:

''(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 112 of the Federal Information Security Modernization Act of 2022;

''(F) Federal and non-Federal cyber threat intelligence;

''(G) data on compliance with 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.'';

(4) in subsection (d)(2)—

(A) in the paragraph heading, by striking ''NOTICE AND COMMENT'' and inserting ''CONSULTATION, NOTICE, AND COMMENT'';

(B) by inserting ''promulgate,'' before ''significantly modify''; and

(C) by striking ''shall be made after the public is given an opportunity to comment on

the Director's proposed decision.'' and inserting ''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.''; and

(5) by adding at the end the following:

''(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 Of-

fice 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.

''(C) REQUIREMENTS BURDEN REDUCTION AND CLARITY.—In conducting the review described in subparagraph (A), the Director shall consider—

''(i) the cumulative reporting and compliance burden to agencies; and

''(ii) the clarity of the requirements and deadlines contained in guidance and policy documents.

''(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 60 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.''.

SEC. 105. ACTIONS TO ENHANCE FEDERAL INCIDENT TRANSPARENCY.

(a) RESPONSIBILITIES OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Director

of the Cybersecurity and Infrastructure Security Agency shall—

(A) develop a plan for the development of the analysis required under section 3597(a) of title 44, United States Code, as added by this title, and the report required under subsection (b) of that section that includes—

(i) a description of any challenges the Director of the Cybersecurity and Infrastructure Security Agency anticipates encountering; and

(ii) the use of automation and machine-readable formats for collecting, compiling, monitoring, and analyzing data; and

(B) provide to the appropriate congressional committees a briefing on the plan developed under subparagraph (A).

(2) BRIEFING.—Not later than 1 year after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall provide to the appropriate congressional committees a briefing on—

(A) the execution of the plan required under paragraph (1)(A); and

(B) the development of the report required under section 3597(b) of title 44, United States Code, as added by this title.

(b) RESPONSIBILITIES OF THE DIRECTOR OF THE OFFICE OF MANAGEMENT AND BUDGET.—

(1) FISMA.—Section 2 of the Federal Information Security Modernization Act of 2014 (44 U.S.C. 3554 note) is amended—

(A) by striking subsection (b); and

(B) by redesignating subsections (c) through (f) as subsections (b) through (e), respectively.

(2) INCIDENT DATA SHARING.—

(A) IN GENERAL.—The Director shall develop guidance, to be updated not less frequently than once every 2 years, on the content, timeliness, and format of the information provided by agencies under section 3594(a) of title 44, United States Code, as added by this title.

(B) REQUIREMENTS.—The guidance developed under subparagraph (A) shall—

(i) prioritize the availability of data necessary to understand and analyze—

(I) the causes of incidents;

(II) the scope and scale of incidents within the environments and systems of an agency;

(III) a root cause analysis of incidents that—

(aa) are common across the Federal Government; or

(bb) have a Government-wide impact;

(IV) agency response, recovery, and remediation actions and the effectiveness of those actions; and

(V) the impact of incidents;

(ii) enable the efficient development of—

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

(II) the report on Federal incidents required under section 3597(b) of title 44, United States Code, as added by this title;

(iii) include requirements for the timeliness of data production; and

(iv) include requirements for using automation and machine-readable data for data sharing and availability.

(3) GUIDANCE ON RESPONDING TO INFORMATION REQUESTS.—Not later than 1 year after the date of enactment of this Act, the Director shall develop guidance for agencies to implement the requirement under section 3594(c) of title 44, United States Code, as added by this title, to provide information to other agencies experiencing incidents.

(4) STANDARD GUIDANCE AND TEMPLATES.—Not later than 1 year after the date of enactment of this Act, the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, shall develop guidance and templates, to be reviewed and, if necessary, updated not less frequently than once every 2 years, for use by Federal agencies in the activities required under sections 3592, 3593, and 3596 of title 44, United States Code, as added by this title.

(5) CONTRACTOR AND AWARDEE GUIDANCE.—

(A) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Director, in coordination with the Secretary of Homeland Security, the Secretary of Defense,

the Administrator of General Services, and the heads of other agencies determined appropriate by the Director, shall issue guidance to Federal agencies on how to deconflict, to the greatest extent practicable, existing regulations, policies, and procedures relating to the responsibilities of contractors and awardees established under section 3595 of title 44, United States Code, as added by this title.

(B) EXISTING PROCESSES.—To the greatest extent practicable, the guidance issued under subparagraph (A) shall allow contractors and awardees to use existing processes for notifying Federal agencies of incidents involving information of the Federal Government.

(6) UPDATED BRIEFINGS.—Not less frequently than once every 2 years, the Director shall provide to the appropriate congressional committees an update on the guidance and templates developed under paragraphs (2) through (4).

(c) UPDATE TO THE PRIVACY ACT OF 1974.—Section 552a(b) of title 5, United States Code (commonly known as the ''Privacy Act of 1974'') is amended—

(1) in paragraph (11), by striking ''or'' at the end;

(2) in paragraph (12), by striking the period at the end and inserting ''; or''; and

(3) by adding at the end the following:

''(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.''.

SEC. 106. ADDITIONAL GUIDANCE TO AGENCIES ON FISMA UPDATES.

Not later than 1 year after the date of enactment of this Act, the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, shall issue guidance for agencies on—

(1) performing the ongoing and continuous agency system risk assessment required under section 3554(a)(1)(A) of title 44, United States Code, as amended by this title;

(2) implementing additional cybersecurity procedures, which shall include resources for shared services;

(3) establishing a process for providing the status of each remedial action under section 3554(b)(7) of title 44, United States Code, as amended by this title, to the Director and the Cybersecurity and Infrastructure Security Agency using automation and machine-readable data, as practicable, which shall include—

(A) specific guidance for the use of automation and machine-readable data; and

(B) templates for providing the status of the remedial action; and

(4) a requirement to coordinate with inspectors general of agencies to ensure consistent understanding and application of agency policies for the purpose of evaluations by inspectors general.

SEC. 107. AGENCY REQUIREMENTS TO NOTIFY PRIVATE SECTOR ENTITIES IMPACTED BY INCIDENTS.

(a) DEFINITIONS.—In this section:

(1) REPORTING ENTITY.—The term ''reporting entity'' means private organization or governmental unit that is required by statute or regulation to submit sensitive information to an agency.

(2) SENSITIVE INFORMATION.—The term ''sensitive information'' has the meaning given the term

by the Director in guidance issued under subsection (b).

(b) GUIDANCE ON NOTIFICATION OF REPORTING ENTITIES.—Not later than 180 days after the date of enactment of this Act, the Director shall issue guidance requiring the head of each agency to notify a reporting entity of an incident that is likely to substantially affect—

(1) the confidentiality or integrity of sensitive information submitted by the reporting entity to the agency pursuant to a statutory or regulatory requirement; or

(2) the agency information system or systems used in the transmission or storage of the sensitive information described in paragraph (1).

SEC. 108. MOBILE SECURITY STANDARDS.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Director shall—

(1) evaluate mobile application security guidance promulgated by the Director; and

(2) issue guidance to secure mobile devices, including for mobile applications, for every agency.

(b) CONTENTS.—The guidance issued under subsection (a)(2) shall include—

(1) a requirement, pursuant to section 3506(b)(4) of title 44, United States Code, for every

agency to maintain a continuous inventory of every—

(A) mobile device operated by or on behalf of the agency; and

(B) vulnerability identified by the agency associated with a mobile device; and

(2) a requirement for every agency to perform continuous evaluation of the vulnerabilities described in paragraph (1)(B) and other risks associated with the use of applications on mobile devices.

(c) INFORMATION SHARING.—The Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall issue guidance to agencies for sharing the inventory of the agency required under subsection (b)(1) with the Director of the Cybersecurity and Infrastructure Security Agency, using automation and machine-readable data to the greatest extent practicable.

(d) BRIEFING.—Not later than 60 days after the date on which the Director issues guidance under subsection (a)(2), the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall provide to the appropriate congressional committees a briefing on the guidance.

SEC. 109. DATA AND LOGGING RETENTION FOR INCIDENT RESPONSE.

(a) RECOMMENDATIONS.—Not later than 2 years after the date of enactment of this Act, and not less frequently than every 2 years thereafter, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Attorney General, shall submit to the Director recommendations on requirements for logging events on agency systems and retaining other relevant data within the systems and networks of an agency.

(b) CONTENTS.—The recommendations provided under subsection (a) shall include—

(1) the types of logs to be maintained;

(2) the duration that logs and other relevant data should be retained;

(3) the time periods for agency implementation of recommended logging and security requirements;

(4) how to ensure the confidentiality, integrity, and availability of logs;

(5) requirements to ensure that, upon request, 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), agencies provide logs to—

(A) the Director of the Cybersecurity and Infrastructure Security Agency for a cybersecurity purpose; and

(B) the Director of the Federal Bureau of Investigation, or the appropriate Federal law enforcement agency, to investigate potential criminal activity; and

(6) requirements to ensure that, subject to compliance with statistical laws and other relevant data protection requirements, the highest level security operations center of each agency has visibility into all agency logs.

(c) GUIDANCE.—Not later than 90 days after receiving the recommendations submitted under subsection (a), the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the Attorney General, shall, as determined to be appropriate by the Director, update guidance to agencies regarding requirements for logging, log retention, log management, sharing of log data with other appropriate agencies, or any other logging activity determined to be appropriate by the Director.

(d) SUNSET.—This section shall cease to have force or effect on the date that is 10 years after the date of the enactment of this Act.

SEC. 110. CISA AGENCY ADVISORS.

(a) IN GENERAL.—Not later than 120 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall assign not less than 1 cybersecurity professional employed by the Cybersecurity and Infrastructure Security Agency to be the Cybersecurity and Infrastructure Security Agency advisor to the senior agency information security officer of each agency.

(b) QUALIFICATIONS.—Each advisor assigned under subsection (a) shall have knowledge of—

(1) cybersecurity threats facing agencies, including any specific threats to the assigned agency;

(2) performing risk assessments of agency systems; and

(3) other Federal cybersecurity initiatives.

(c) DUTIES.—The duties of each advisor assigned under subsection (a) shall include—

(1) providing ongoing assistance and advice, as requested, to the agency Chief Information Officer;

(2) serving as an incident response point of contact between the assigned agency and the Cybersecurity and Infrastructure Security Agency; and

(3) familiarizing themselves with agency systems, processes, and procedures to better facilitate support to the agency in responding to incidents.

(d) LIMITATION.—An advisor assigned under subsection (a) shall not be a contractor.

(e) MULTIPLE ASSIGNMENTS.—One individual advisor may be assigned to multiple agency Chief Information Officers under subsection (a).

SEC. 111. FEDERAL PENETRATION TESTING POLICY.

(a) IN GENERAL.—Subchapter II of chapter 35 of title 44, United States Code, is amended by adding at the end the following:

"§ 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, in consultation with the Secretary, acting through the Director of the Cybersecurity and Infrastructure Security Agency, shall issue guidance to agencies that—

''(A) requires agencies to use, when and where appropriate, penetration testing on agen-

cy systems by both Federal and non-Federal entities; 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, including 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).''.

(b) DEADLINE FOR GUIDANCE.—Not later than 180 days after the date of enactment of this Act, the Director

shall issue the guidance required under section 3559A(b) of title 44, United States Code, as added by subsection (a).

(c) CLERICAL AMENDMENT.—The table of sections for chapter 35 of title 44, United States Code, is amended by adding after the item relating to section 3559 the following:

''3559A. Federal penetration testing.''.

(d) SUNSET.—

(1) IN GENERAL.—Effective on the date that is 10 years after the date of enactment of this Act, subchapter II of chapter 35 of title 44, United States Code, is amended by striking section 3559A.

(2) CLERICAL AMENDMENT.—Effective on the date that is 10 years after the date of enactment of this Act, the table of sections for chapter 35 of title 44, United States Code, is amended by striking the item relating to section 3559A.

SEC. 112. ONGOING THREAT HUNTING PROGRAM.

(a) THREAT HUNTING PROGRAM.—

(1) IN GENERAL.—Not later than 540 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall establish a program to provide ongoing, hypothesis-driven threat-hunting services on the network of each agency.

(2) PLAN.—Not later than 180 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall develop a plan to establish the program required under paragraph (1) that describes how the Director of the Cybersecurity and Infrastructure Security Agency plans to—

(A) determine the method for collecting, storing, accessing, analyzing, and safeguarding appropriate agency data;

(B) provide on-premises support to agencies;

(C) staff threat hunting services;

(D) allocate available human and financial resources to implement the plan; and

(E) provide input to the heads of agencies on the use of—

(i) more stringent standards under section 11331(c)(1) of title 40, United States Code; and

(ii) additional cybersecurity procedures under section 3554 of title 44, United States Code.

(b) REPORTS.—The Director of the Cybersecurity and Infrastructure Security Agency shall submit to the appropriate congressional committees—

(1) not later than 30 days after the date on which the Director of the Cybersecurity and Infrastructure Security Agency completes the plan required under subsection (a)(2), a report on the plan to provide threat hunting services to agencies;

(2) not less than 30 days before the date on which the Director of the Cybersecurity and Infrastructure Security Agency begins providing threat hunting services under the program under subsection (a)(1), a report providing any updates to the plan developed under subsection (a)(2); and

(3) not later than 1 year after the date on which the Director of the Cybersecurity and Infrastructure Security Agency begins providing threat hunting services to agencies other than the Cybersecurity and Infrastructure Security Agency, a report describing lessons learned from providing those services.

SEC. 113. CODIFYING VULNERABILITY DISCLOSURE PROGRAMS.

(a) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by inserting after section 3559A, as added by section 111 of this title, the following:

"§ 3559B. Federal vulnerability disclosure programs

''(a) PURPOSE; SENSE OF CONGRESS.—

''(1) PURPOSE.—The purpose of Federal vulnerability disclosure programs is to create a mechanism to use the expertise of the public to provide a service to Federal agencies by identifying information system vulnerabilities.

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

''(b) DEFINITIONS.—In this section:

''(1) 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.

''(c) 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 (e)(2); and

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

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

mation 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 Director of 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 (e)(2).

''(d) 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.

''(e) 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 and cover every internet accessible Federal information system

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.

''(f) CONGRESSIONAL REPORTING.—Not later than 90 days after the date of enactment of the Federal Information Security Modernization Act of 2022, and annually thereafter for a 3-year period, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with 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 (c)(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).''.

(b) CLERICAL AMENDMENT.—The table of sections for chapter 35 of title 44, United States Code, is amended by adding after the item relating to section 3559A, as added by section 111, the following:

''3559B. Federal vulnerability disclosure programs.''.

(c) SUNSET.—

(1) IN GENERAL.—Effective on the date that is 10 years after the date of enactment of this Act, subchapter II of chapter 35 of title 44, United States Code, is amended by striking section 3559B.

(2) CLERICAL AMENDMENT.—Effective on the date that is 10 years after the date of enactment of this Act, the table of sections for chapter 35 of title 44, United States Code, is amended by striking the item relating to section 3559B.

SEC. 114. IMPLEMENTING ZERO TRUST ARCHITECTURE.

(a) GUIDANCE.—Not later than 18 months after the date of enactment of this Act, the Director shall provide an update to the appropriate congressional committees on progress in increasing the internal defenses of agency systems, including—

(1) shifting away from ''trusted networks'' to implement security controls based on a presumption of compromise;

(2) implementing principles of least privilege in administering information security programs;

(3) limiting the ability of entities that cause incidents to move laterally through or between agency systems;

(4) identifying incidents quickly;

(5) isolating and removing unauthorized entities from agency systems as quickly as practicable, accounting for intelligence or law enforcement purposes;

(6) otherwise increasing the resource costs for entities that cause incidents to be successful; and

(7) a summary of the agency progress reports required under subsection (b).

(b) AGENCY PROGRESS REPORTS.—Not later than 270 days after the date of enactment of this Act, the head of each agency shall submit to the Director a progress re-

port on implementing an information security program based on the presumption of compromise and least privilege principles, which shall include—

(1) a description of any steps the agency has completed, including progress toward achieving requirements issued by the Director, including the adoption of any models or reference architecture;

(2) an identification of activities that have not yet been completed and that would have the most immediate security impact; and

(3) a schedule to implement any planned activities.

SEC. 115. AUTOMATION REPORTS.

(a) OMB REPORT.—Not later than 180 days after the date of enactment of this Act, the Director shall provide to the appropriate congressional committees an update on the use of automation under paragraphs (1), (5)(C), and (8)(B) of section 3554(b) of title 44, United States Code.

(b) GAO REPORT.—Not later than 1 year after the date of enactment of this Act, the Comptroller General of the United States shall perform a study on the use of automation and machine readable data across the Federal Government for cybersecurity purposes, including the

automated updating of cybersecurity tools, sensors, or processes by agencies.

SEC. 116. EXTENSION OF FEDERAL ACQUISITION SECURITY COUNCIL AND SOFTWARE INVENTORY.

(a) EXTENSION.—Section 1328 of title 41, United States Code, is amended by striking ''the date that'' and all that follows and inserting ''December 31, 2026.''.

(b) REQUIREMENT.—Subsection 1326(b) of title 41, United States Code, is amended—

(1) in paragraph (5), by striking ''and'' at the end;

(2) by redesignating paragraph (6) as paragraph (7); and

(3) by inserting after paragraph (5) the following:

''(6) maintaining an up-to-date and accurate inventory of software in use by the agency and, if available and applicable, the components of such software, that can be communicated at the request of the Federal Acquisition Security Council, the National Cyber Director, or the Secretary of Homeland Security, acting through the Director of Cybersecurity and Infrastructure Security Agency; and''.

SEC. 117. COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY DASHBOARD.

(a) DASHBOARD REQUIRED.—Section 11(e)(2) of the Inspector General Act of 1978 (5 U.S.C. App.) is amended—

(1) in subparagraph (A), by striking ''and'' at the end;

(2) by redesignating subparagraph (B) as subparagraph (C); and

(3) by inserting after subparagraph (A) the following:

''(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''.

SEC. 118. QUANTITATIVE CYBERSECURITY METRICS.

(a) DEFINITION OF COVERED METRICS.—In this section, the term ''covered metrics'' means the metrics established, reviewed, and updated under section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c)).

(b) UPDATING AND ESTABLISHING METRICS.—Not later than 1 year after the date of enactment of this Act, and as appropriate thereafter, the Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Director, shall—

(1) evaluate any covered metrics established as of the date of enactment of this Act; and

(2) as appropriate and pursuant to section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c)) update or establish new covered metrics.

(c) IMPLEMENTATION.—

(1) IN GENERAL.—Not later than 540 days after the date of enactment of this Act, the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall promulgate guidance that requires each agency to use covered metrics to track trends in the cybersecurity and incident response capabilities of the agency.

(2) PERFORMANCE DEMONSTRATION.—The guidance issued under paragraph (1) and any subsequent guidance shall require agencies to share with the Director of the Cybersecurity and Infrastructure Security Agency data demonstrating the performance of the agency using the covered metrics included in the guidance.

(3) PENETRATION TESTS.—On not less than 2 occasions during the 2-year period following the date on which guidance is promulgated under paragraph (1), the Director shall ensure that not less than 3 agencies are subjected to substantially similar pene-

tration tests, as determined by the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, in order to validate the utility of the covered metrics.

(4) ANALYSIS CAPACITY.—The Director of the Cybersecurity and Infrastructure Security Agency shall develop a capability that allows for the analysis of the covered metrics, including cross-agency performance of agency cybersecurity and incident response capability trends.

(5) TIME-BASED METRIC.—With respect the first update or establishment of covered metrics required under subsection (b)(2), the Director of the Cybersecurity and Infrastructure Security Agency shall establish covered metrics that include not less than 1 metric addressing the time it takes for agencies to identify and respond to incidents.

(d) CONGRESSIONAL REPORTS.—Not later than 1 year after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Director, shall submit to the appropriate congressional committees a report on the utility and use of the covered metrics.

SEC. 119. ESTABLISHMENT OF RISK-BASED BUDGET MODEL.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

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

(B) the Committee on Oversight and Reform, the Committee on Homeland Security, and the Committee on Appropriations of the House of Representatives.

(2) COVERED AGENCY.—The term ''covered agency'' has the meaning given the term ''executive agency'' in section 133 of title 41, United States Code.

(3) DIRECTOR.—The term ''Director'' means the Director of the Office of Management and Budget.

(4) INFORMATION TECHNOLOGY.—The term ''information technology''—

(A) has the meaning given the term in section 11101 of title 40, United States Code; and

(B) includes the hardware and software systems of a Federal agency that monitor and

control physical equipment and processes of the Federal agency.

(5) RISK-BASED BUDGET.—The term ''risk-based budget'' means a budget—

(A) developed by identifying and prioritizing cybersecurity risks and vulnerabilities, including impact on agency operations in the case of a cyber attack, through analysis of cyber threat intelligence, incident data, and tactics, techniques, procedures, and capabilities of cyber threats; and

(B) that allocates resources based on the risks identified and prioritized under subparagraph (A).

(b) ESTABLISHMENT OF RISK-BASED BUDGET MODEL.—

(1) IN GENERAL.—

(A) MODEL.—Not later than 1 year after the first publication of the budget submitted by the President under section 1105 of title 31, United States Code, following the date of enactment of this Act, the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director and in coordination with the Di-

rector of the National Institute of Standards and Technology, shall develop a standard model for informing a risk-based budget for cybersecurity spending.

(B) RESPONSIBILITY OF DIRECTOR.—Section 3553(a) of title 44, United States Code, as amended by section 103 of this title, is further amended by inserting after paragraph (6) the following:

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

(C) CONTENTS OF MODEL.—The model required to be developed under subparagraph (A) shall utilize appropriate information to evaluate risk, including, as determined appropriate by the Director—

(i) Federal and non-Federal cyber threat intelligence products, where available, to identify threats, vulnerabilities, and risks;

(ii) analysis of the impact of agency operations of compromise of systems, including the interconnectivity to other agen-

cy systems and the operations of other agencies; and

(iii) to the greatest extent practicable, analysis of where resources should be allocated to have the greatest impact on mitigating current and future threats and current and future cybersecurity capabilities.

(D) USE OF MODEL.—The model required to be developed under subparagraph (A) shall be used to—

(i) inform acquisition and sustainment of—

(I) information technology and cybersecurity tools;

(II) information technology and cybersecurity architectures;

(III) information technology and cybersecurity personnel; and

(IV) cybersecurity and information technology concepts of operations; and

(ii) evaluate and inform Government-wide cybersecurity programs.

(E) MODEL VARIATION.—The Director may develop multiple models under subpara-

graph (A) based on different agency characteristics, such as size or cybersecurity maturity.

(F) REQUIRED UPDATES.—Not less frequently than once every 3 years, the Director shall review, and update as necessary, the model required to be developed under subparagraph (A).

(G) PUBLICATION.—Not earlier than 5 years after the date on which the model developed under subparagraph (A) is completed, the Director shall, taking into account any classified or sensitive information, publish the model, and any updates necessary under subparagraph (F), on the public website of the Office of Management and Budget.

(H) REPORTS.—Not later than 2 years after the first publication of the budget submitted by the President under section 1105 of title 31, United States Code, following the date of enactment of this Act, and annually thereafter for each of the 2 following fiscal years or until the date on which the model required to be developed under subparagraph (A) is completed, whichever is sooner, the Director shall submit to the appropriate congressional com-

mittees a report on the development of the model.

(2) PHASED IMPLEMENTATION OF RISK-BASED BUDGET MODEL.—

(A) INITIAL PHASE.—

(i) IN GENERAL.—Not later than 2 years after the date on which the model developed under paragraph (1) is completed, the Director shall require not less than 5 covered agencies to use the model to inform the development of the annual cybersecurity and information technology budget requests of those covered agencies.

(ii) BRIEFING.—Not later than 1 year after the date on which the covered agencies selected under clause (i) begin using the model developed under paragraph (1), the Director shall provide to the appropriate congressional committees a briefing on implementation of risk-based budgeting for cybersecurity spending, an assessment of agency implementation, and an evaluation of whether the risk-based budget helps to mitigate cybersecurity vulnerabilities.

(B) FULL DEPLOYMENT.—Not later than 5 years after the date on which the model developed under paragraph (1) is completed, the head of each covered agency shall use the model, or any updated model pursuant to paragraph (1)(F), to the greatest extent practicable, to inform the development of the annual cybersecurity and information technology budget requests of the covered agency.

(C) AGENCY PERFORMANCE PLANS.—

(i) AMENDMENT.—Section 3554(d)(2) of title 44, United States Code, is amended by inserting ''and the risk-based budget model required under section 3553(a)(7)'' after ''paragraph (1)''.

(ii) EFFECTIVE DATE.—The amendment made by clause (i) shall take effect on the date that is 5 years after the date on which the model developed under paragraph (1) is completed.

(3) VERIFICATION.—

(A) IN GENERAL.—Section 1105(a)(35)(A)(i) of title 31, United States Code, is amended—

(i) in the matter preceding subclause (I), by striking ''by agency, and by initiative area (as determined by the administration)'' and inserting ''and by agency'';

(ii) in subclause (III), by striking ''and'' at the end; and

(iii) by adding at the end the following:

''(V) a validation that the budgets submitted were informed by 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.''.

(B) EFFECTIVE DATE.—The amendments made by subparagraph (A) shall take effect on the date that is 5 years after the date on which the model developed under paragraph (1) is completed.

(4) REPORTS.—

(A) INDEPENDENT EVALUATION.—Section 3555(a)(2) of title 44, United States Code, is amended—

(i) in subparagraph (B), by striking ''and'' at the end;

(ii) in subparagraph (C), by striking the period at the end and inserting ''; and''; and

(iii) by adding at the end the following:

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

(B) ASSESSMENT.—

(i) AMENDMENT.—Section 3553(c) of title 44, United States Code, as amended by section 103 of this title, is further amended by inserting after paragraph (5) the following:

''(6) an assessment of—

''(A) Federal agency utilization of the model required under subsection (a)(7); and

''(B) whether the model mitigates the cyber vulnerabilities of the Federal Government.''.

(ii) EFFECTIVE DATE.—The amendment made by clause (i) shall take effect on the date that is 5 years after the date on which the model developed under paragraph (1) is completed.

(5) GAO REPORT.—Not later than 3 years after the date on which the first budget of the President is submitted to Congress containing the validation required under section 1105(a)(35)(A)(i)(V) of title 31, United States Code, as amended by paragraph (3), the Comptroller General of the United States shall submit to the appropriate congressional committees a report that includes—

(A) an evaluation of the success of covered agencies in utilizing the risk-based budget model;

(B) an evaluation of the success of covered agencies in implementing risk-based budgets;

(C) an evaluation of whether the risk-based budgets developed by covered agencies are effective at informing Federal Government-wide cybersecurity programs; and

(D) any other information relating to risk-based budgets the Comptroller General determines appropriate.

SEC. 120. ACTIVE CYBER DEFENSIVE STUDY.

(a) DEFINITION.—In this section, the term ''active defense technique''—

(1) means an action taken on the systems of an entity to increase the security of information on the network of an agency by misleading an adversary; and

(2) includes a honeypot, deception, or purposefully feeding false or misleading data to an adversary when the adversary is on the systems of the entity.

(b) STUDY.—Not later than 180 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Director and the National Cyber Director, shall perform a study on the use of active defense techniques to enhance the security of agencies, which shall include—

(1) a review of legal restrictions on the use of different active cyber defense techniques in Federal environments, in consultation with the Department of Justice;

(2) an evaluation of—

(A) the efficacy of a selection of active defense techniques determined by the Director of the Cybersecurity and Infrastructure Security Agency; and

(B) factors that impact the efficacy of the active defense techniques evaluated under subparagraph (A);

(3) recommendations on safeguards and procedures that shall be established to require that active defense techniques are adequately coordinated to ensure that active defense techniques do not impede agency operations and mission delivery, threat response efforts, criminal investigations, and national security activities, including intelligence collection; and

(4) the development of a framework for the use of different active defense techniques by agencies.

SEC. 121. SECURITY OPERATIONS CENTER AS A SERVICE PILOT.

(a) PURPOSE.—The purpose of this section is for the Cybersecurity and Infrastructure Security Agency 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.

(b) PLAN.—Not later than 1 year after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall develop a plan to establish a centralized Federal security operations cen-

ter shared service offering within the Cybersecurity and Infrastructure Security Agency.

(c) CONTENTS.—The plan required under subsection (b) shall include considerations for—

(1) collecting, organizing, and analyzing agency information system data in real time;

(2) staffing and resources; and

(3) appropriate interagency agreements, concepts of operations, and governance plans.

(d) PILOT PROGRAM.—

(1) IN GENERAL.—Not later than 180 days after the date on which the plan required under subsection (b) is developed, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director, shall enter into a 1-year agreement with not less than 2 agencies to offer a security operations center as a shared service.

(2) ADDITIONAL AGREEMENTS.—After the date on which the briefing required under subsection (e)(1) is provided, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director, may enter into additional 1-year agreements described in paragraph (1) with agencies.

(e) BRIEFING AND REPORT.—

(1) BRIEFING.—Not later than 270 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Oversight and Reform of the House of Representatives a briefing on the parameters of any 1-year agreements entered into under subsection (d)(1).

(2) REPORT.—Not later than 90 days after the date on which the first 1-year agreement entered into under subsection (d) expires, the Director of the Cybersecurity and Infrastructure Security Agency shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Oversight and Reform of the House of Representatives a report on—

(A) the agreement; and

(B) any additional agreements entered into with agencies under subsection (d).

SEC. 122. EXTENSION OF CHIEF DATA OFFICER COUNCIL.

Section 3520A(e)(2) of title 44, United States Code, is amended by striking ''upon the expiration of the 2-year

period that begins on the date the Comptroller General submits the report under paragraph (1) to Congress'' and inserting ''January 31, 2030''.

TITLE II—CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022

SEC. 201. SHORT TITLE.

This title may be cited as the ''Cyber Incident Reporting for Critical Infrastructure Act of 2022''.

SEC. 202. DEFINITIONS.

In this title:

(1) COVERED CYBER INCIDENT; COVERED ENTITY; CYBER INCIDENT; INFORMATION SYSTEM; RANSOM PAYMENT; RANSOMWARE ATTACK; SECURITY VULNERABILITY.—The terms ''covered cyber incident'', ''covered entity'', ''cyber incident'', ''information system'', ''ransom payment'', ''ransomware attack'', and ''security vulnerability'' have the meanings given those terms in section 2240 of the Homeland Security Act of 2002, as added by section 203 of this title.

(2) DIRECTOR.—The term ''Director'' means the Director of the Cybersecurity and Infrastructure Security Agency.

SEC. 203. CYBER INCIDENT REPORTING.

(a) CYBER INCIDENT REPORTING.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(1) in section 2209(c) (6 U.S.C. 659(c))—

(A) in paragraph (11), by striking ''; and'' and inserting a semicolon;

(B) in paragraph (12), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(13) receiving, aggregating, and analyzing reports related to covered cyber incidents (as defined in section 2240) submitted by covered entities (as defined in section 2240) and reports related to ransom payments (as defined in section 2240) submitted by covered entities (as defined in section 2240) in furtherance of the activities specified in sections 2202(e), 2203, and 2241, this subsection, and any other authorized activity of the Director, to enhance the situational awareness of cybersecurity threats across critical infrastructure sectors.''; and

(2) by adding at the end the following:

''Subtitle D—Cyber Incident Reporting

''SEC. 2240. DEFINITIONS.

''In this subtitle:

''(1) CENTER.—The term 'Center' means the center established under section 2209.

''(2) CLOUD SERVICE PROVIDER.—The term 'cloud service provider' means an entity offering products or services related to cloud computing, as defined by the National Institute of Standards and Technology in NIST Special Publication 800–145 and any amendatory or superseding document relating thereto.

''(3) COUNCIL.—The term 'Council' means the Cyber Incident Reporting Council described in section 2246.

''(4) COVERED CYBER INCIDENT.—The term 'covered cyber incident' means a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the final rule issued pursuant to section 2242(b).

''(5) COVERED ENTITY.—The term 'covered entity' means an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21, that satisfies the definition established by the Director in the final rule issued pursuant to section 2242(b).

''(6) CYBER INCIDENT.—The term 'cyber incident'—

''(A) has the meaning given the term 'incident' in section 2209; and

''(B) does not include an occurrence that imminently, but not actually, jeopardizes—

''(i) information on information systems; or

''(ii) information systems.

''(7) CYBER THREAT.—The term 'cyber threat' has the meaning given the term 'cybersecurity threat' in section 2201.

''(8) CYBER THREAT INDICATOR; CYBERSECURITY PURPOSE; DEFENSIVE MEASURE; FEDERAL ENTITY; SECURITY VULNERABILITY.—The terms 'cyber threat indicator', 'cybersecurity purpose', 'defensive measure', 'Federal entity', and 'security vulnerability' have the meanings given those terms in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

''(9) INCIDENT; SHARING.—The terms 'incident' and 'sharing' have the meanings given those terms in section 2209.

''(10) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term 'Information Sharing

and Analysis Organization' has the meaning given the term in section 2222.

''(11) INFORMATION SYSTEM.—The term 'information system'—

''(A) has the meaning given the term in section 3502 of title 44, United States Code; and

''(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

''(12) MANAGED SERVICE PROVIDER.—The term 'managed service provider' means an entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer, in the data center of the entity (such as hosting), or in a third party data center.

''(13) RANSOM PAYMENT.—The term 'ransom payment' means the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack.

''(14) RANSOMWARE ATTACK.—The term 'ransomware attack'—

''(A) means an incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment; and

''(B) does not include any such event where the demand for payment is—

''(i) not genuine; or

''(ii) made in good faith by an entity in response to a specific request by the owner or operator of the information system.

''(15) SECTOR RISK MANAGEMENT AGENCY.—The term 'Sector Risk Management Agency' has the meaning given the term in section 2201.

''(16) SIGNIFICANT CYBER INCIDENT.—The term 'significant cyber incident' means a cyber inci-

dent, or a group of related cyber incidents, that the Secretary determines is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States.

''(17) SUPPLY CHAIN COMPROMISE.—The term 'supply chain compromise' means an incident within the supply chain of an information system that an adversary can leverage or does leverage to jeopardize the confidentiality, integrity, or availability of the information system or the information the system processes, stores, or transmits, and can occur at any point during the life cycle.

''(18) VIRTUAL CURRENCY.—The term 'virtual currency' means the digital representation of value that functions as a medium of exchange, a unit of account, or a store of value.

''(19) VIRTUAL CURRENCY ADDRESS.—The term 'virtual currency address' means a unique public cryptographic key identifying the location to which a virtual currency payment can be made.

''SEC. 2241. CYBER INCIDENT REVIEW.

''(a) ACTIVITIES.—The Center shall—

''(1) receive, aggregate, analyze, and secure, using processes consistent with the processes developed pursuant to the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.) reports from covered entities related to a covered cyber incident to assess the effectiveness of security controls, identify tactics, techniques, and procedures adversaries use to overcome those controls and other cybersecurity purposes, including to assess potential impact of cyber incidents on public health and safety and to enhance situational awareness of cyber threats across critical infrastructure sectors;

''(2) coordinate and share information with appropriate Federal departments and agencies to identify and track ransom payments, including those utilizing virtual currencies;

''(3) leverage information gathered about cyber incidents to—

''(A) enhance the quality and effectiveness of information sharing and coordination efforts with appropriate entities, including agencies, sector coordinating councils, Information Sharing and Analysis Organizations, State, local, Tribal, and territorial governments, technology providers, critical infrastructure owners and op-

erators, cybersecurity and cyber incident response firms, and security researchers; and

''(B) provide appropriate entities, including sector coordinating councils, Information Sharing and Analysis Organizations, State, local, Tribal, and territorial governments, technology providers, cybersecurity and cyber incident response firms, and security researchers, with timely, actionable, and anonymized reports of cyber incident campaigns and trends, including, to the maximum extent practicable, related contextual information, cyber threat indicators, and defensive measures, pursuant to section 2245;

''(4) establish mechanisms to receive feedback from stakeholders on how the Agency can most effectively receive covered cyber incident reports, ransom payment reports, and other voluntarily provided information, and how the Agency can most effectively support private sector cybersecurity;

''(5) facilitate the timely sharing, on a voluntary basis, between relevant critical infrastructure owners and operators of information relating to covered cyber incidents and ransom payments, particularly with respect to ongoing cyber threats or security vulnerabilities and identify and disseminate

ways to prevent or mitigate similar cyber incidents in the future;

''(6) for a covered cyber incident, including a ransomware attack, that also satisfies the definition of a significant cyber incident, or is part of a group of related cyber incidents that together satisfy such definition, conduct a review of the details surrounding the covered cyber incident or group of those incidents and identify and disseminate ways to prevent or mitigate similar incidents in the future;

''(7) with respect to covered cyber incident reports under section 2242(a) and 2243 involving an ongoing cyber threat or security vulnerability, immediately review those reports for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to appropriate stakeholders, in coordination with other divisions within the Agency, as appropriate;

''(8) publish quarterly unclassified, public reports that describe aggregated, anonymized observations, findings, and recommendations based on covered cyber incident reports, which may be based on the unclassified information contained in the briefings required under subsection (c);

''(9) proactively identify opportunities, consistent with the protections in section 2245, to leverage and utilize data on cyber incidents in a manner that enables and strengthens cybersecurity research carried out by academic institutions and other private sector organizations, to the greatest extent practicable; and

''(10) in accordance with section 2245 and subsection (b) of this section, as soon as possible but not later than 24 hours after receiving a covered cyber incident report, ransom payment report, voluntarily submitted information pursuant to section 2243, or information received pursuant to a request for information or subpoena under section 2244, make available the information to appropriate Sector Risk Management Agencies and other appropriate Federal agencies.

''(b) INTERAGENCY SHARING.—The President or a designee of the President—

''(1) may establish a specific time requirement for sharing information under subsection (a)(11); and

''(2) shall determine the appropriate Federal agencies under subsection (a)(11).

''(c) PERIODIC BRIEFING.—Not later than 60 days after the effective date of the final rule required under section 2242(b), and on the first day of each month thereafter, the Director, in consultation with the National Cyber Director, the Attorney General, and the Director of National Intelligence, shall provide to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a briefing that characterizes the national cyber threat landscape, including the threat facing Federal agencies and covered entities, and applicable intelligence and law enforcement information, covered cyber incidents, and ransomware attacks, as of the date of the briefing, which shall—

''(1) include the total number of reports submitted under sections 2242 and 2243 during the preceding month, including a breakdown of required and voluntary reports;

''(2) include any identified trends in covered cyber incidents and ransomware attacks over the course of the preceding month and as compared to previous reports, including any trends related to the

information collected in the reports submitted under sections 2242 and 2243, including—

''(A) the infrastructure, tactics, and techniques malicious cyber actors commonly use; and

''(B) intelligence gaps that have impeded, or currently are impeding, the ability to counter covered cyber incidents and ransomware threats;

''(3) include a summary of the known uses of the information in reports submitted under sections 2242 and 2243; and

''(4) include an unclassified portion, but may include a classified component.

''SEC. 2242. REQUIRED REPORTING OF CERTAIN CYBER INCIDENTS.

''(a) IN GENERAL.—

''(1) COVERED CYBER INCIDENT REPORTS.—

''(A) IN GENERAL.—A covered entity that experiences a covered cyber incident shall report the covered cyber incident to the Agency not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.

''(B) LIMITATION.—The Director may not require reporting under subparagraph (A) any earlier than 72 hours after the covered entity reasonably believes that a covered cyber incident has occurred.

''(2) RANSOM PAYMENT REPORTS.—

''(A) IN GENERAL.—A covered entity that makes a ransom payment as the result of a ransomware attack against the covered entity shall report the payment to the Agency not later than 24 hours after the ransom payment has been made.

''(B) APPLICATION.—The requirements under subparagraph (A) shall apply even if the ransomware attack is not a covered cyber incident subject to the reporting requirements under paragraph (1).

''(3) SUPPLEMENTAL REPORTS.—A covered entity shall promptly submit to the Agency an update or supplement to a previously submitted covered cyber incident report if substantial new or different information becomes available or if the covered entity makes a ransom payment after submitting a covered cyber incident report required under paragraph (1), until such date that such covered entity notifies

the Agency that the covered cyber incident at issue has concluded and has been fully mitigated and resolved.

''(4) PRESERVATION OF INFORMATION.—Any covered entity subject to requirements of paragraph (1), (2), or (3) shall preserve data relevant to the covered cyber incident or ransom payment in accordance with procedures established in the final rule issued pursuant to subsection (b).

''(5) EXCEPTIONS.—

''(A) REPORTING OF COVERED CYBER INCIDENT WITH RANSOM PAYMENT.—If a covered entity is the victim of a covered cyber incident and makes a ransom payment prior to the 72 hour requirement under paragraph (1), such that the reporting requirements under paragraphs (1) and (2) both apply, the covered entity may submit a single report to satisfy the requirements of both paragraphs in accordance with procedures established in the final rule issued pursuant to subsection (b).

''(B) SUBSTANTIALLY SIMILAR REPORTED INFORMATION.—

''(i) IN GENERAL.—Subject to the limitation described in clause (ii), where

the Agency has an agreement in place that satisfies the requirements of section 4(a) of the Cyber Incident Reporting for Critical Infrastructure Act of 2022, the requirements under paragraphs (1), (2), and (3) shall not apply to a covered entity required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe.

''(ii) LIMITATION.—The exemption in clause (i) shall take effect with respect to a covered entity once an agency agreement and sharing mechanism is in place between the Agency and the respective Federal agency, pursuant to section 4(a) of the Cyber Incident Reporting for Critical Infrastructure Act of 2022.

''(iii) RULES OF CONSTRUCTION.—Nothing in this paragraph shall be construed to—

''(I) exempt a covered entity from the reporting requirements under paragraph (3) unless the supplemental report also meets the re-

quirements of clauses (i) and (ii) of this paragraph;

"(II) prevent the Agency from contacting an entity submitting information to another Federal agency that is provided to the Agency pursuant to section 4 of the Cyber Incident Reporting for Critical Infrastructure Act of 2022; or

"(III) prevent an entity from communicating with the Agency.

"(C) DOMAIN NAME SYSTEM.—The requirements under paragraphs (1), (2) and (3) shall not apply to a covered entity or the functions of a covered entity that the Director determines constitute critical infrastructure owned, operated, or governed by multi-stakeholder organizations that develop, implement, and enforce policies concerning the Domain Name System, such as the Internet Corporation for Assigned Names and Numbers or the Internet Assigned Numbers Authority.

"(6) MANNER, TIMING, AND FORM OF REPORTS.—Reports made under paragraphs (1), (2), and (3) shall be made in the manner and form, and

within the time period in the case of reports made under paragraph (3), prescribed in the final rule issued pursuant to subsection (b).

''(7) EFFECTIVE DATE.—Paragraphs (1) through (4) shall take effect on the dates prescribed in the final rule issued pursuant to subsection (b).

''(b) RULEMAKING.—

''(1) NOTICE OF PROPOSED RULEMAKING.—Not later than 24 months after the date of enactment of this section, the Director, in consultation with Sector Risk Management Agencies, the Department of Justice, and other Federal agencies, shall publish in the Federal Register a notice of proposed rulemaking to implement subsection (a).

''(2) FINAL RULE.—Not later than 18 months after publication of the notice of proposed rulemaking under paragraph (1), the Director shall issue a final rule to implement subsection (a).

''(3) SUBSEQUENT RULEMAKINGS.—

''(A) IN GENERAL.—The Director is authorized to issue regulations to amend or revise the final rule issued pursuant to paragraph (2).

''(B) PROCEDURES.—Any subsequent rules issued under subparagraph (A) shall comply with the requirements under chapter 5 of title

5, United States Code, including the issuance of a notice of proposed rulemaking under section 553 of such title.

''(c) ELEMENTS.—The final rule issued pursuant to subsection (b) shall be composed of the following elements:

''(1) A clear description of the types of entities that constitute covered entities, based on—

''(A) the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety;

''(B) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and

''(C) the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure.

''(2) A clear description of the types of substantial cyber incidents that constitute covered cyber incidents, which shall—

''(A) at a minimum, require the occurrence of—

''(i) a cyber incident that leads to substantial loss of confidentiality, integrity, or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes;

''(ii) a disruption of business or industrial operations, including due to a denial of service attack, ransomware attack, or exploitation of a zero day vulnerability, against

''(I) an information system or network; or

''(II) an operational technology system or process; or

''(iii) unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise;

''(B) consider—

"(i) the sophistication or novelty of the tactics used to perpetrate such a cyber incident, as well as the type, volume, and sensitivity of the data at issue;

"(ii) the number of individuals directly or indirectly affected or potentially affected by such a cyber incident; and

"(iii) potential impacts on industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers; and

"(C) exclude—

"(i) any event where the cyber incident is perpetrated in good faith by an entity in response to a specific request by the owner or operator of the information system; and

"(ii) the threat of disruption as extortion, as described in section 2240(14)(A).

"(3) A requirement that, if a covered cyber incident or a ransom payment occurs following an exempted threat described in paragraph (2)(C)(ii), the covered entity shall comply with the requirements in

this subtitle in reporting the covered cyber incident or ransom payment.

''(4) A clear description of the specific required contents of a report pursuant to subsection (a)(1), which shall include the following information, to the extent applicable and available, with respect to a covered cyber incident:

''(A) A description of the covered cyber incident, including—

''(i) identification and a description of the function of the affected information systems, networks, or devices that were, or are reasonably believed to have been, affected by such cyber incident;

''(ii) a description of the unauthorized access with substantial loss of confidentiality, integrity, or availability of the affected information system or network or disruption of business or industrial operations;

''(iii) the estimated date range of such incident; and

''(iv) the impact to the operations of the covered entity.

''(B) Where applicable, a description of the vulnerabilities exploited and the security defenses that were in place, as well as the tactics, techniques, and procedures used to perpetrate the covered cyber incident.

''(C) Where applicable, any identifying or contact information related to each actor reasonably believed to be responsible for such cyber incident.

''(D) Where applicable, identification of the category or categories of information that were, or are reasonably believed to have been, accessed or acquired by an unauthorized person.

''(E) The name and other information that clearly identifies the covered entity impacted by the covered cyber incident, including, as applicable, the State of incorporation or formation of the covered entity, trade names, legal names, or other identifiers.

''(F) Contact information, such as telephone number or electronic mail address, that the Agency may use to contact the covered entity or an authorized agent of such covered entity, or, where applicable, the service provider of

such covered entity acting with the express permission of, and at the direction of, the covered entity to assist with compliance with the requirements of this subtitle.

''(5) A clear description of the specific required contents of a report pursuant to subsection (a)(2), which shall be the following information, to the extent applicable and available, with respect to a ransom payment:

''(A) A description of the ransomware attack, including the estimated date range of the attack.

''(B) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetrate the ransomware attack.

''(C) Where applicable, any identifying or contact information related to the actor or actors reasonably believed to be responsible for the ransomware attack.

''(D) The name and other information that clearly identifies the covered entity that made the ransom payment or on whose behalf the payment was made.

''(E) Contact information, such as telephone number or electronic mail address, that the Agency may use to contact the covered entity that made the ransom payment or an authorized agent of such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission of, and at the direction of, that covered entity to assist with compliance with the requirements of this subtitle.

''(F) The date of the ransom payment.

''(G) The ransom payment demand, including the type of virtual currency or other commodity requested, if applicable.

''(H) The ransom payment instructions, including information regarding where to send the payment, such as the virtual currency address or physical address the funds were requested to be sent to, if applicable.

''(I) The amount of the ransom payment.

''(6) A clear description of the types of data required to be preserved pursuant to subsection (a)(4), the period of time for which the data is required to be preserved, and allowable uses, processes, and procedures.

''(7) Deadlines and criteria for submitting supplemental reports to the Agency required under subsection (a)(3), which shall—

''(A) be established by the Director in consultation with the Council;

''(B) consider any existing regulatory reporting requirements similar in scope, purpose, and timing to the reporting requirements to which such a covered entity may also be subject, and make efforts to harmonize the timing and contents of any such reports to the maximum extent practicable;

''(C) balance the need for situational awareness with the ability of the covered entity to conduct cyber incident response and investigations; and

''(D) provide a clear description of what constitutes substantial new or different information.

''(8) Procedures for—

''(A) entities, including third parties pursuant to subsection (d)(1), to submit reports required by paragraphs (1), (2), and (3) of subsection (a), including the manner and form

thereof, which shall include, at a minimum, a concise, user-friendly web-based form;

''(B) the Agency to carry out—

''(i) the enforcement provisions of section 2244, including with respect to the issuance, service, withdrawal, referral process, and enforcement of subpoenas, appeals and due process procedures;

''(ii) other available enforcement mechanisms including acquisition, suspension and debarment procedures; and

''(iii) other aspects of noncompliance;

''(C) implementing the exceptions provided in subsection (a)(5); and

''(D) protecting privacy and civil liberties consistent with processes adopted pursuant to section 105(b) of the Cybersecurity Act of 2015 (6 U.S.C. 1504(b)) and anonymizing and safeguarding, or no longer retaining, information received and disclosed through covered cyber incident reports and ransom payment reports that is known to be personal information of a specific individual or information that identifies a specific individual that is not directly related to a cybersecurity threat.

''(9) Other procedural measures directly necessary to implement subsection (a).

''(d) THIRD PARTY REPORT SUBMISSION AND RANSOM PAYMENT.—

''(1) REPORT SUBMISSION.—A covered entity that is required to submit a covered cyber incident report or a ransom payment report may use a third party, such as an incident response company, insurance provider, service provider, Information Sharing and Analysis Organization, or law firm, to submit the required report under subsection (a).

''(2) RANSOM PAYMENT.—If a covered entity impacted by a ransomware attack uses a third party to make a ransom payment, the third party shall not be required to submit a ransom payment report for itself under subsection (a)(2).

''(3) DUTY TO REPORT.—Third-party reporting under this subparagraph does not relieve a covered entity from the duty to comply with the requirements for covered cyber incident report or ransom payment report submission.

''(4) RESPONSIBILITY TO ADVISE.—Any third party used by a covered entity that knowingly makes a ransom payment on behalf of a covered entity impacted by a ransomware attack shall advise the im-

pacted covered entity of the responsibilities of the impacted covered entity regarding reporting ransom payments under this section.

''(e) OUTREACH TO COVERED ENTITIES.—

''(1) IN GENERAL.—The Agency shall conduct an outreach and education campaign to inform likely covered entities, entities that offer or advertise as a service to customers to make or facilitate ransom payments on behalf of covered entities impacted by ransomware attacks and other appropriate entities of the requirements of paragraphs (1), (2), and (3) of subsection (a).

''(2) ELEMENTS.—The outreach and education campaign under paragraph (1) shall include the following:

''(A) An overview of the final rule issued pursuant to subsection (b).

''(B) An overview of mechanisms to submit to the Agency covered cyber incident reports, ransom payment reports, and information relating to the disclosure, retention, and use of covered cyber incident reports and ransom payment reports under this section.

''(C) An overview of the protections afforded to covered entities for complying with

the requirements under paragraphs (1), (2), and (3) of subsection (a).

''(D) An overview of the steps taken under section 2244 when a covered entity is not in compliance with the reporting requirements under subsection (a).

''(E) Specific outreach to cybersecurity vendors, cyber incident response providers, cybersecurity insurance entities, and other entities that may support covered entities.

''(F) An overview of the privacy and civil liberties requirements in this subtitle.

''(3) COORDINATION.—In conducting the outreach and education campaign required under paragraph (1), the Agency may coordinate with—

''(A) the Critical Infrastructure Partnership Advisory Council established under section 871;

''(B) Information Sharing and Analysis Organizations;

''(C) trade associations;

''(D) information sharing and analysis centers;

''(E) sector coordinating councils; and

''(F) any other entity as determined appropriate by the Director.

''(f) EXEMPTION.—Sections 3506(c), 3507, 3508, and 3509 of title 44, United States Code, shall not apply to any action to carry out this section.

''(g) RULE OF CONSTRUCTION.—Nothing in this section shall affect the authorities of the Federal Government to implement the requirements of Executive Order 14028 (86 Fed. Reg. 26633; relating to improving the nation's cybersecurity), including changes to the Federal Acquisition Regulations and remedies to include suspension and debarment.

''(h) SAVINGS PROVISION.—Nothing in this section shall be construed to supersede or to abrogate, modify, or otherwise limit the authority that is vested in any officer or any agency of the United States Government to regulate or take action with respect to the cybersecurity of an entity.

''SEC. 2243. VOLUNTARY REPORTING OF OTHER CYBER INCIDENTS.

''(a) IN GENERAL.—Entities may voluntarily report cyber incidents or ransom payments to the Agency that are not required under paragraph (1), (2), or (3) of section 2242(a), but may enhance the situational awareness of cyber threats.

''(b) VOLUNTARY PROVISION OF ADDITIONAL INFORMATION IN REQUIRED REPORTS.—Covered entities may voluntarily include in reports required under paragraph (1), (2), or (3) of section 2242(a) information that is not required to be included, but may enhance the situational awareness of cyber threats.

''(c) APPLICATION OF PROTECTIONS.—The protections under section 2245 applicable to reports made under section 2242 shall apply in the same manner and to the same extent to reports and information submitted under subsections (a) and (b).

''SEC. 2244. NONCOMPLIANCE WITH REQUIRED REPORTING.

''(a) PURPOSE.—In the event that a covered entity that is required to submit a report under section 2242(a) fails to comply with the requirement to report, the Director may obtain information about the cyber incident or ransom payment by engaging the covered entity directly to request information about the cyber incident or ransom payment, and if the Director is unable to obtain information through such engagement, by issuing a subpoena to the covered entity, pursuant to subsection (c), to gather information sufficient to determine whether a covered cyber incident or ransom payment has occurred.

''(b) INITIAL REQUEST FOR INFORMATION.—

''(1) IN GENERAL.—If the Director has reason to believe, whether through public reporting or other information in the possession of the Federal Government, including through analysis performed pursuant to paragraph (1) or (2) of section 2241(a), that a covered entity has experienced a covered cyber incident or made a ransom payment but failed to report such cyber incident or payment to the Agency in accordance with section 2242(a), the Director may request additional information from the covered entity to confirm whether or not a covered cyber incident or ransom payment has occurred.

''(2) TREATMENT.—Information provided to the Agency in response to a request under paragraph (1) shall be treated as if it was submitted through the reporting procedures established in section 2242.

''(c) ENFORCEMENT.—

''(1) IN GENERAL.—If, after the date that is 72 hours from the date on which the Director made the request for information in subsection (b), the Director has received no response from the covered entity from which such information was requested, or received an inadequate response, the Director may issue to such covered entity a subpoena to compel disclosure of information the Director deems nec-

essary to determine whether a covered cyber incident or ransom payment has occurred and obtain the information required to be reported pursuant to section 2242 and any implementing regulations, and assess potential impacts to national security, economic security, or public health and safety.

''(2) CIVIL ACTION.—

''(A) IN GENERAL.—If a covered entity fails to comply with a subpoena, the Director may refer the matter to the Attorney General to bring a civil action in a district court of the United States to enforce such subpoena.

''(B) VENUE.—An action under this paragraph may be brought in the judicial district in which the covered entity against which the action is brought resides, is found, or does business.

''(C) CONTEMPT OF COURT.—A court may punish a failure to comply with a subpoena issued under this subsection as contempt of court.

''(3) NON-DELEGATION.—The authority of the Director to issue a subpoena under this subsection may not be delegated.

''(4) AUTHENTICATION.—

"(A) IN GENERAL.—Any subpoena issued electronically pursuant to this subsection shall be authenticated with a cryptographic digital signature of an authorized representative of the Agency, or other comparable successor technology, that allows the Agency to demonstrate that such subpoena was issued by the Agency and has not been altered or modified since such issuance.

"(B) INVALID IF NOT AUTHENTICATED.—Any subpoena issued electronically pursuant to this subsection that is not authenticated in accordance with subparagraph (A) shall not be considered to be valid by the recipient of such subpoena.

"(d) PROVISION OF CERTAIN INFORMATION TO ATTORNEY GENERAL.—

"(1) IN GENERAL.—Notwithstanding section 2245(a)(5) and paragraph (b)(2) of this section, if the Director determines, based on the information provided in response to a subpoena issued pursuant to subsection (c), that the facts relating to the cyber incident or ransom payment at issue may constitute grounds for a regulatory enforcement action or criminal prosecution, the Director may provide such

information to the Attorney General or the head of the appropriate Federal regulatory agency, who may use such information for a regulatory enforcement action or criminal prosecution.

''(2) CONSULTATION.—The Director may consult with the Attorney General or the head of the appropriate Federal regulatory agency when making the determination under paragraph (1).

''(e) CONSIDERATIONS.—When determining whether to exercise the authorities provided under this section, the Director shall take into consideration—

''(1) the complexity in determining if a covered cyber incident has occurred; and

''(2) prior interaction with the Agency or awareness of the covered entity of the policies and procedures of the Agency for reporting covered cyber incidents and ransom payments.

''(f) EXCLUSIONS.—This section shall not apply to a State, local, Tribal, or territorial government entity.

''(g) REPORT TO CONGRESS.—The Director shall submit to Congress an annual report on the number of times the Director—

''(1) issued an initial request for information pursuant to subsection (b);

''(2) issued a subpoena pursuant to subsection (c); or

''(3) referred a matter to the Attorney General for a civil action pursuant to subsection (c)(2).

''(h) PUBLICATION OF THE ANNUAL REPORT.—The Director shall publish a version of the annual report required under subsection (g) on the website of the Agency, which shall include, at a minimum, the number of times the Director—

''(1) issued an initial request for information pursuant to subsection (b); or

''(2) issued a subpoena pursuant to subsection (c).

''(i) ANONYMIZATION OF REPORTS.—The Director shall ensure any victim information contained in a report required to be published under subsection (h) be anonymized before the report is published.

''SEC. 2245. INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.

''(a) DISCLOSURE, RETENTION, AND USE.—

''(1) AUTHORIZED ACTIVITIES.—Information provided to the Agency pursuant to section 2242 or 2243 may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department,

component, officer, employee, or agent of the Federal Government solely for—

"(A) a cybersecurity purpose;

"(B) the purpose of identifying—

"(i) a cyber threat, including the source of the cyber threat; or

"(ii) a security vulnerability;

"(C) the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or use of a weapon of mass destruction;

"(D) the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

"(E) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a cyber incident reported pursuant to section 2242 or 2243 or any of the offenses listed in section 105(d)(5)(A)(v) of the Cybersecurity Act of 2015 (6 U.S.C. 1504(d)(5)(A)(v)).

''(2) AGENCY ACTIONS AFTER RECEIPT.—

''(A) RAPID, CONFIDENTIAL SHARING OF CYBER THREAT INDICATORS.—Upon receiving a covered cyber incident or ransom payment report submitted pursuant to this section, the Agency shall immediately review the report to determine whether the cyber incident that is the subject of the report is connected to an ongoing cyber threat or security vulnerability and where applicable, use such report to identify, develop, and rapidly disseminate to appropriate stakeholders actionable, anonymized cyber threat indicators and defensive measures.

''(B) PRINCIPLES FOR SHARING SECURITY VULNERABILITIES.—With respect to information in a covered cyber incident or ransom payment report regarding a security vulnerability referred to in paragraph (1)(B)(ii), the Director shall develop principles that govern the timing and manner in which information relating to security vulnerabilities may be shared, consistent with common industry best practices and United States and international standards.

''(3) PRIVACY AND CIVIL LIBERTIES.—Information contained in covered cyber incident and ransom

payment reports submitted to the Agency pursuant to section 2242 shall be retained, used, and disseminated, where permissible and appropriate, by the Federal Government in accordance with processes to be developed for the protection of personal information consistent with processes adopted pursuant to section 105 of the Cybersecurity Act of 2015 (6 U.S.C. 1504) and in a manner that protects from unauthorized use or disclosure any information that may contain—

''(A) personal information of a specific individual that is not directly related to a cybersecurity threat; or

''(B) information that identifies a specific individual that is not directly related to a cybersecurity threat.

''(4) DIGITAL SECURITY.—The Agency shall ensure that reports submitted to the Agency pursuant to section 2242, and any information contained in those reports, are collected, stored, and protected at a minimum in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication 199, or any successor document.

''(5) PROHIBITION ON USE OF INFORMATION IN REGULATORY ACTIONS.—

''(A) IN GENERAL.—A Federal, State, local, or Tribal government shall not use information about a covered cyber incident or ransom payment obtained solely through reporting directly to the Agency in accordance with this subtitle to regulate, including through an enforcement action, the activities of the covered entity or entity that made a ransom payment, unless the government entity expressly allows entities to submit reports to the Agency to meet regulatory reporting obligations of the entity.

''(B) CLARIFICATION.—A report submitted to the Agency pursuant to section 2242 or 2243 may, consistent with Federal or State regulatory authority specifically relating to the prevention and mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to such systems.

''(b) PROTECTIONS FOR REPORTING ENTITIES AND INFORMATION.—Reports describing covered cyber incidents or ransom payments submitted to the Agency by entities in accordance with section 2242, as well as volun-

tarily-submitted cyber incident reports submitted to the Agency pursuant to section 2243, shall—

''(1) be considered the commercial, financial, and proprietary information of the covered entity when so designated by the covered entity;

''(2) be exempt from disclosure under section 552(b)(3) of title 5, United States Code (commonly known as the 'Freedom of Information Act'), as well as any provision of State, Tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records;

''(3) be considered not to constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection; and

''(4) not be subject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.

''(c) LIABILITY PROTECTIONS.—

''(1) IN GENERAL.—No cause of action shall lie or be maintained in any court by any person or entity and any such action shall be promptly dismissed for the submission of a report pursuant to section 2242(a) that is submitted in conformance with this

subtitle and the rule promulgated under section 2242(b), except that this subsection shall not apply with regard to an action by the Federal Government pursuant to section 2244(c)(2).

''(2) SCOPE.—The liability protections provided in this subsection shall only apply to or affect litigation that is solely based on the submission of a covered cyber incident report or ransom payment report to the Agency.

''(3) RESTRICTIONS.—Notwithstanding paragraph (2), no report submitted to the Agency pursuant to this subtitle or any communication, document, material, or other record, created for the sole purpose of preparing, drafting, or submitting such report, may be received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, provided that nothing in this subtitle shall create a defense to discovery or otherwise affect the discovery of any communication, document, material, or other record not created for the sole purpose of preparing, drafting, or submitting such report.

''(d) SHARING WITH NON-FEDERAL ENTITIES.—The Agency shall anonymize the victim who reported the information when making information provided in reports received under section 2242 available to critical infrastructure owners and operators and the general public.

''(e) STORED COMMUNICATIONS ACT.—Nothing in this subtitle shall be construed to permit or require disclosure by a provider of a remote computing service or a provider of an electronic communication service to the public of information not otherwise permitted or required to be disclosed under chapter 121 of title 18, United States Code (commonly known as the 'Stored Communications Act').

''SEC. 2246. CYBER INCIDENT REPORTING COUNCIL.

''(a) RESPONSIBILITY OF THE SECRETARY.—The Secretary shall lead an intergovernmental Cyber Incident Reporting Council, in consultation with the Director of the Office of Management and Budget, the Attorney General, the National Director Cyber Director, Sector Risk Management Agencies, and other appropriate Federal agencies, to coordinate, deconflict, and harmonize Federal incident reporting requirements, including those issued through regulations.

''(b) RULE OF CONSTRUCTION.—Nothing in subsection (a) shall be construed to provide any additional regulatory authority to any Federal entity.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended by inserting after the items relating to subtitle C of title XXII the following:

''Subtitle D—Cyber Incident Reporting

''Sec. 2240. Definitions.
''Sec. 2241. Cyber Incident Review.
''Sec. 2242. Required reporting of certain cyber incidents.
''Sec. 2243. Voluntary reporting of other cyber incidents.
''Sec. 2244. Noncompliance with required reporting.
''Sec. 2245. Information shared with or provided to the Federal Government.
''Sec. 2246. Cyber Incident Reporting Council.''.

SEC. 204. FEDERAL SHARING OF INCIDENT REPORTS.

(a) CYBER INCIDENT REPORTING SHARING.—

(1) IN GENERAL.—Notwithstanding any other provision of law or regulation, any Federal agency, including any independent establishment (as defined in section 104 of title 5, United States Code), that receives a report from an entity of a cyber incident, including a ransomware attack, shall provide the report to the Agency as soon as possible, but not later than 24 hours after receiving the report, unless a shorter period is required by an agreement made between the Department of Homeland Security (including the Cybersecurity and Infrastructure Secu-

rity Agency) and the recipient Federal agency. The Director shall share and coordinate each report pursuant to section 2241(b) of the Homeland Security Act of 2002, as added by section 203 of this title.

(2) RULE OF CONSTRUCTION.—The requirements described in paragraph (1) and section 2245(d) of the Homeland Security Act of 2002, as added by section 203 of this title, may not be construed to be a violation of any provision of law or policy that would otherwise prohibit disclosure or provision of information within the executive branch.

(3) PROTECTION OF INFORMATION.—The Director shall comply with any obligations of the recipient Federal agency described in paragraph (1) to protect information, including with respect to privacy, confidentiality, or information security, if those obligations would impose greater protection requirements than this Act or the amendments made by this Act.

(4) EFFECTIVE DATE.—This subsection shall take effect on the effective date of the final rule issued pursuant to section 2242(b) of the Homeland Security Act of 2002, as added by section 203 of this title.

(5) AGENCY AGREEMENTS.—

(A) IN GENERAL.—The Agency and any Federal agency, including any independent establishment (as defined in section 104 of title 5, United States Code) that receives incident reports from entities, including due to ransomware attacks, shall, as appropriate, enter into a documented agreement to establish policies, processes, procedures, and mechanisms to ensure reports are shared with the Agency pursuant to paragraph (1).

(B) AVAILABILITY.—To the maximum extent practicable, each documented agreement required under subparagraph (A) shall be made publicly available.

(C) REQUIREMENT.—The documented agreements required by subparagraph (A) shall require reports be shared from Federal agencies with the Agency in such time as to meet the overall timeline for covered entity reporting of covered cyber incidents and ransom payments established in section 2242 of the Homeland Security Act of 2002, as added by section 203 of this title.

(b) HARMONIZING REPORTING REQUIREMENTS.—The Secretary of Homeland Security, acting through the

Director, shall, in consultation with the Cyber Incident Reporting Council described in section 2246 of the Homeland Security Act of 2002, as added by section 203 of this title, to the maximum extent practicable—

(1) periodically review existing regulatory requirements, including the information required in such reports, to report incidents and ensure that any such reporting requirements and procedures avoid conflicting, duplicative, or burdensome requirements; and

(2) coordinate with appropriate Federal partners and regulatory authorities that receive reports relating to incidents to identify opportunities to streamline reporting processes, and where feasible, facilitate interagency agreements between such authorities to permit the sharing of such reports, consistent with applicable law and policy, without impacting the ability of the Agency to gain timely situational awareness of a covered cyber incident or ransom payment.

SEC. 205. RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM.

(a) PROGRAM.—Not later than 1 year after the date of enactment of this Act, the Director shall establish a ransomware vulnerability warning pilot program to lever-

age existing authorities and technology to specifically develop processes and procedures for, and to dedicate resources to, identifying information systems that contain security vulnerabilities associated with common ransomware attacks, and to notify the owners of those vulnerable systems of their security vulnerability.

(b) IDENTIFICATION OF VULNERABLE SYSTEMS.—The pilot program established under subsection (a) shall—

(1) identify the most common security vulnerabilities utilized in ransomware attacks and mitigation techniques; and

(2) utilize existing authorities to identify information systems that contain the security vulnerabilities identified in paragraph (1).

(c) ENTITY NOTIFICATION.—

(1) IDENTIFICATION.—If the Director is able to identify the entity at risk that owns or operates a vulnerable information system identified in subsection (b), the Director may notify the owner of the information system.

(2) NO IDENTIFICATION.—If the Director is not able to identify the entity at risk that owns or operates a vulnerable information system identified in subsection (b), the Director may utilize the subpoena authority pursuant to section 2209 of the Homeland

Security Act of 2002 (6 U.S.C. 659) to identify and notify the entity at risk pursuant to the procedures under that section.

(3) REQUIRED INFORMATION.—A notification made under paragraph (1) shall include information on the identified security vulnerability and mitigation techniques.

(d) PRIORITIZATION OF NOTIFICATIONS.—To the extent practicable, the Director shall prioritize covered entities for identification and notification activities under the pilot program established under this section.

(e) LIMITATION ON PROCEDURES.—No procedure, notification, or other authorities utilized in the execution of the pilot program established under subsection (a) shall require an owner or operator of a vulnerable information system to take any action as a result of a notice of a security vulnerability made pursuant to subsection (c).

(f) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide additional authorities to the Director to identify vulnerabilities or vulnerable systems.

(g) TERMINATION.—The pilot program established under subsection (a) shall terminate on the date that is 4 years after the date of enactment of this Act.

SEC. 206. RANSOMWARE THREAT MITIGATION ACTIVITIES.

(a) JOINT RANSOMWARE TASK FORCE.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Director, in consultation with the National Cyber Director, the Attorney General, and the Director of the Federal Bureau of Investigation, shall establish and chair the Joint Ransomware Task Force to coordinate an ongoing nationwide campaign against ransomware attacks, and identify and pursue opportunities for international cooperation.

(2) COMPOSITION.—The Joint Ransomware Task Force shall consist of participants from Federal agencies, as determined appropriate by the National Cyber Director in consultation with the Secretary of Homeland Security.

(3) RESPONSIBILITIES.—The Joint Ransomware Task Force, utilizing only existing authorities of each participating Federal agency, shall coordinate across the Federal Government the following activities:

(A) Prioritization of intelligence-driven operations to disrupt specific ransomware actors.

(B) Consult with relevant private sector, State, local, Tribal, and territorial governments and international stakeholders to identify needs

and establish mechanisms for providing input into the Joint Ransomware Task Force.

(C) Identifying, in consultation with relevant entities, a list of highest threat ransomware entities updated on an ongoing basis, in order to facilitate—

(i) prioritization for Federal action by appropriate Federal agencies; and

(ii) identify metrics for success of said actions.

(D) Disrupting ransomware criminal actors, associated infrastructure, and their finances.

(E) Facilitating coordination and collaboration between Federal entities and relevant entities, including the private sector, to improve Federal actions against ransomware threats.

(F) Collection, sharing, and analysis of ransomware trends to inform Federal actions.

(G) Creation of after-action reports and other lessons learned from Federal actions that identify successes and failures to improve subsequent actions.

(H) Any other activities determined appropriate by the Joint Ransomware Task Force to mitigate the threat of ransomware attacks.

(b) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide any additional authority to any Federal agency.

SEC. 207. CONGRESSIONAL REPORTING.

(a) REPORT ON STAKEHOLDER ENGAGEMENT.—Not later than 30 days after the date on which the Director issues the final rule under section 2242(b) of the Homeland Security Act of 2002, as added by section 203(b) of this title, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report that describes how the Director engaged stakeholders in the development of the final rule.

(b) REPORT ON OPPORTUNITIES TO STRENGTHEN SECURITY RESEARCH.—Not later than 1 year after the date of enactment of this Act, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report describing how the National Cybersecurity and Communications Integration Center established under section 2209

of the Homeland Security Act of 2002 (6 U.S.C. 659) has carried out activities under section 2241(a)(9) of the Homeland Security Act of 2002, as added by section 203(a) of this title, by proactively identifying opportunities to use cyber incident data to inform and enable cybersecurity research within the academic and private sector.

(c) REPORT ON RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM.—Not later than 1 year after the date of enactment of this Act, and annually thereafter for the duration of the pilot program established under section 205, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report, which may include a classified annex, on the effectiveness of the pilot program, which shall include a discussion of the following:

(1) The effectiveness of the notifications under section 205(c) in mitigating security vulnerabilities and the threat of ransomware.

(2) Identification of the most common vulnerabilities utilized in ransomware.

(3) The number of notifications issued during the preceding year.

(4) To the extent practicable, the number of vulnerable devices or systems mitigated under the

pilot program by the Agency during the preceding year.

(d) REPORT ON HARMONIZATION OF REPORTING REGULATIONS.—

(1) IN GENERAL.—Not later than 180 days after the date on which the Secretary of Homeland Security convenes the Cyber Incident Reporting Council described in section 2246 of the Homeland Security Act of 2002, as added by section 203 of this title, the Secretary of Homeland Security shall submit to the appropriate congressional committees a report that includes—

(A) a list of duplicative Federal cyber incident reporting requirements on covered entities;

(B) a description of any challenges in harmonizing the duplicative reporting requirements;

(C) any actions the Director intends to take to facilitate harmonizing the duplicative reporting requirements; and

(D) any proposed legislative changes necessary to address the duplicative reporting.

(2) RULE OF CONSTRUCTION.—Nothing in paragraph (1) shall be construed to provide any additional regulatory authority to any Federal agency.

(e) GAO REPORTS.—

(1) IMPLEMENTATION OF THIS ACT.—Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the implementation of this Act and the amendments made by this Act.

(2) EXEMPTIONS TO REPORTING.—Not later than 1 year after the date on which the Director issues the final rule required under section 2242(b) of the Homeland Security Act of 2002, as added by section 203 of this title, the Comptroller General of the United States shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the exemptions to reporting under paragraphs (2) and (5) of section 2242(a) of the Homeland Security Act of 2002, as added by section 203 of this title, which shall include—

(A) to the extent practicable, an evaluation of the quantity of cyber incidents not reported to the Federal Government;

(B) an evaluation of the impact on impacted entities, homeland security, and the national economy due to cyber incidents, ransomware attacks, and ransom payments, including a discussion on the scope of impact of cyber incidents that were not reported to the Federal Government;

(C) an evaluation of the burden, financial and otherwise, on entities required to report cyber incidents under this Act, including an analysis of entities that meet the definition of a small business concern under section 3 of the Small Business Act (15 U.S.C. 632); and

(D) a description of the consequences and effects of limiting covered cyber incident and ransom payment reporting to only covered entities.

(f) REPORT ON EFFECTIVENESS OF ENFORCEMENT MECHANISMS.—Not later than 1 year after the date on which the Director issues the final rule required under section 2242(b) of the Homeland Security Act of 2002, as added by section 203 of this title, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on

the effectiveness of the enforcement mechanisms within section 2244 of the Homeland Security Act of 2002, as added by section 203 of this title.

TITLE III—FEDERAL SECURE CLOUD IMPROVEMENT AND JOBS ACT OF 2022

SEC. 301. SHORT TITLE.

This title may be cited as the ''Federal Secure Cloud Improvement and Jobs Act of 2022''.

SEC. 302. FINDINGS.

Congress finds the following:

(1) Ensuring that the Federal Government can securely leverage cloud computing products and services is key to expediting the modernization of legacy information technology systems, increasing cybersecurity within and across departments and agencies, and supporting the continued leadership of the United States in technology innovation and job creation.

(2) According to independent analysis, as of calendar year 2019, the size of the cloud computing market had tripled since 2004, enabling more than 2,000,000 jobs and adding more than $200,000,000,000 to the gross domestic product of the United States.

(3) The Federal Government, across multiple presidential administrations and Congresses, has continued to support the ability of agencies to move to the cloud, including through—

(A) President Barack Obama's ''Cloud First Strategy'';

(B) President Donald Trump's ''Cloud Smart Strategy'';

(C) the prioritization of cloud security in Executive Order 14028 (86 Fed. Reg. 26633; relating to improving the nation's cybersecurity), which was issued by President Joe Biden; and

(D) more than a decade of appropriations and authorization legislation that provides agencies with relevant authorities and appropriations to modernize on-premises information technology systems and more readily adopt cloud computing products and services.

(4) Since it was created in 2011, the Federal Risk and Authorization Management Program (referred to in this section as ''FedRAMP'') at the General Services Administration has made steady and sustained improvements in supporting the secure authorization and reuse of cloud computing

products and services within the Federal Government, including by reducing the costs and burdens on both agencies and cloud companies to quickly and securely enter the Federal market.

(5) According to data from the General Services Administration, as of the end of fiscal year 2021, there were 239 cloud providers with FedRAMP authorizations, and those authorizations had been reused more than 2,700 times across various agencies.

(6) Providing a legislative framework for FedRAMP and new authorities to the General Services Administration, the Office of Management and Budget, and Federal agencies will—

(A) improve the speed at which new cloud computing products and services can be securely authorized;

(B) enhance the ability of agencies to effectively evaluate FedRAMP authorized providers for reuse;

(C) reduce the costs and burdens to cloud providers seeking a FedRAMP authorization; and

(D) provide for more robust transparency and dialogue between industry and the Federal Government to drive stronger adoption of se-

cure cloud capabilities, create jobs, and reduce wasteful legacy information technology.

SEC. 303. TITLE 44 AMENDMENTS.

(a) AMENDMENT.—Chapter 36 of title 44, United States Code, is amended by adding at the end the following:

"§ 3607. Definitions

''(a) IN GENERAL.—Except as provided under subsection (b), the definitions under sections 3502 and 3552 apply to this section through section 3616.

''(b) ADDITIONAL DEFINITIONS.—In this section through section 3616:

''(1) ADMINISTRATOR.—The term 'Administrator' means the Administrator of General Services.

''(2) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives.

''(3) AUTHORIZATION TO OPERATE; FEDERAL INFORMATION.—The terms 'authorization to operate' and 'Federal information' have the meaning given those term in Circular A–130 of the Office of Management and Budget entitled 'Managing Infor-

mation as a Strategic Resource', or any successor document.

''(4) CLOUD COMPUTING.—The term 'cloud computing' has the meaning given the term in Special Publication 800–145 of the National Institute of Standards and Technology, or any successor document.

''(5) CLOUD SERVICE PROVIDER.—The term 'cloud service provider' means an entity offering cloud computing products or services to agencies.

''(6) FEDRAMP.—The term 'FedRAMP' means the Federal Risk and Authorization Management Program established under section 3608.

''(7) FEDRAMP AUTHORIZATION.—The term 'FedRAMP authorization' means a certification that a cloud computing product or service has—

''(A) completed a FedRAMP authorization process, as determined by the Administrator; or

''(B) received a FedRAMP provisional authorization to operate, as determined by the FedRAMP Board.

''(8) FEDRAMP AUTHORIZATION PACKAGE.—The term 'FedRAMP authorization package' means the essential information that can be used by an agency to determine whether to authorize the oper-

ation of an information system or the use of a designated set of common controls for all cloud computing products and services authorized by FedRAMP.

''(9) FEDRAMP BOARD.—The term 'FedRAMP Board' means the board established under section 3610.

''(10) INDEPENDENT ASSESSMENT SERVICE.—The term 'independent assessment service' means a third-party organization accredited by the Administrator to undertake conformity assessments of cloud service providers and the products or services of cloud service providers.

''(11) SECRETARY.—The term 'Secretary' means the Secretary of Homeland Security.

''§ 3608. Federal Risk and Authorization Management Program

''There is established within the General Services Administration the Federal Risk and Authorization Management Program. The Administrator, subject to section 3614, shall establish a Government-wide program that provides a standardized, reusable approach to security assessment and authorization for cloud computing products and services that process unclassified information used by agencies.

"§ 3609. Roles and responsibilities of the General Services Administration

''(a) ROLES AND RESPONSIBILITIES.—The Administrator shall—

''(1) in consultation with the Secretary, develop, coordinate, and implement a process to support agency review, reuse, and standardization, where appropriate, of security assessments of cloud computing products and services, including, as appropriate, oversight of continuous monitoring of cloud computing products and services, pursuant to guidance issued by the Director pursuant to section 3614;

''(2) establish processes and identify criteria consistent with guidance issued by the Director under section 3614 to make a cloud computing product or service eligible for a FedRAMP authorization and validate whether a cloud computing product or service has a FedRAMP authorization;

''(3) develop and publish templates, best practices, technical assistance, and other materials to support the authorization of cloud computing products and services and increase the speed, effectiveness, and transparency of the authorization process, consistent with standards and guidelines established

by the Director of the National Institute of Standards and Technology and relevant statutes;

''(4) establish and update guidance on the boundaries of FedRAMP authorization packages to enhance the security and protection of Federal information and promote transparency for agencies and users as to which services are included in the scope of a FedRAMP authorization;

''(5) grant FedRAMP authorizations to cloud computing products and services consistent with the guidance and direction of the FedRAMP Board;

''(6) establish and maintain a public comment process for proposed guidance and other FedRAMP directives that may have a direct impact on cloud service providers and agencies before the issuance of such guidance or other FedRAMP directives;

''(7) coordinate with the FedRAMP Board, the Director of the Cybersecurity and Infrastructure Security Agency, and other entities identified by the Administrator, with the concurrence of the Director and the Secretary, to establish and regularly update a framework for continuous monitoring under section 3553;

''(8) provide a secure mechanism for storing and sharing necessary data, including FedRAMP

authorization packages, to enable better reuse of such packages across agencies, including making available any information and data necessary for agencies to fulfill the requirements of section 3613;

''(9) provide regular updates to applicant cloud service providers on the status of any cloud computing product or service during an assessment process;

''(10) regularly review, in consultation with the FedRAMP Board—

''(A) the costs associated with the independent assessment services described in section 3611; and

''(B) the information relating to foreign interests submitted pursuant to section 3612;

''(11) in coordination with the Director of the National Institute of Standards and Technology, the Director, the Secretary, and other stakeholders, as appropriate, determine the sufficiency of underlying standards and requirements to identify and assess the provenance of the software in cloud services and products;

''(12) support the Federal Secure Cloud Advisory Committee established pursuant to section 3616; and

''(13) take such other actions as the Administrator may determine necessary to carry out FedRAMP.

''(b) WEBSITE.—

''(1) IN GENERAL.—The Administrator shall maintain a public website to serve as the authoritative repository for FedRAMP, including the timely publication and updates for all relevant information, guidance, determinations, and other materials required under subsection (a).

''(2) CRITERIA AND PROCESS FOR FEDRAMP AUTHORIZATION PRIORITIES.—The Administrator shall develop and make publicly available on the website described in paragraph (1) the criteria and process for prioritizing and selecting cloud computing products and services that will receive a FedRAMP authorization, in consultation with the FedRAMP Board and the Chief Information Officers Council.

''(c) EVALUATION OF AUTOMATION PROCEDURES.—

''(1) IN GENERAL.—The Administrator, in coordination with the Secretary, shall assess and evaluate available automation capabilities and procedures to improve the efficiency and effectiveness of the issuance of FedRAMP authorizations, including

continuous monitoring of cloud computing products and services.

''(2) MEANS FOR AUTOMATION.—Not later than 1 year after the date of enactment of this section, and updated regularly thereafter, the Administrator shall establish a means for the automation of security assessments and reviews.

''(d) METRICS FOR AUTHORIZATION.—The Administrator shall establish annual metrics regarding the time and quality of the assessments necessary for completion of a FedRAMP authorization process in a manner that can be consistently tracked over time in conjunction with the periodic testing and evaluation process pursuant to section 3554 in a manner that minimizes the agency reporting burden.

"§ 3610. FedRAMP Board

''(a) ESTABLISHMENT.—There is established a FedRAMP Board to provide input and recommendations to the Administrator regarding the requirements and guidelines for, and the prioritization of, security assessments of cloud computing products and services.

''(b) MEMBERSHIP.—The FedRAMP Board shall consist of not more than 7 senior officials or experts from agencies appointed by the Director, in consultation with the Administrator, from each of the following:

''(1) The Department of Defense.

''(2) The Department of Homeland Security.

''(3) The General Services Administration.

''(4) Such other agencies as determined by the Director, in consultation with the Administrator.

''(c) QUALIFICATIONS.—Members of the FedRAMP Board appointed under subsection (b) shall have technical expertise in domains relevant to FedRAMP, such as—

''(1) cloud computing;

''(2) cybersecurity;

''(3) privacy;

''(4) risk management; and

''(5) other competencies identified by the Director to support the secure authorization of cloud services and products.

''(d) DUTIES.—The FedRAMP Board shall—

''(1) in consultation with the Administrator, serve as a resource for best practices to accelerate the process for obtaining a FedRAMP authorization;

''(2) establish and regularly update requirements and guidelines for security authorizations of cloud computing products and services, consistent with standards and guidelines established by the Director of the National Institute of Standards and

Technology, to be used in the determination of FedRAMP authorizations;

''(3) monitor and oversee, to the greatest extent practicable, the processes and procedures by which agencies determine and validate requirements for a FedRAMP authorization, including periodic review of the agency determinations described in section 3613(b);

''(4) ensure consistency and transparency between agencies and cloud service providers in a manner that minimizes confusion and engenders trust; and

''(5) perform such other roles and responsibilities as the Director may assign, with concurrence from the Administrator.

''(e) DETERMINATIONS OF DEMAND FOR CLOUD COMPUTING PRODUCTS AND SERVICES.—The FedRAMP Board may consult with the Chief Information Officers Council to establish a process, which may be made available on the website maintained under section 3609(b), for prioritizing and accepting the cloud computing products and services to be granted a FedRAMP authorization.

''§ 3611. Independent assessment

''The Administrator may determine whether FedRAMP may use an independent assessment service to

analyze, validate, and attest to the quality and compliance of security assessment materials provided by cloud service providers during the course of a determination of whether to use a cloud computing product or service.

"§ 3612. Declaration of foreign interests

''(a) IN GENERAL.—An independent assessment service that performs services described in section 3611 shall annually submit to the Administrator information relating to any foreign interest, foreign influence, or foreign control of the independent assessment service.

''(b) UPDATES.—Not later than 48 hours after there is a change in foreign ownership or control of an independent assessment service that performs services described in section 3611, the independent assessment service shall submit to the Administrator an update to the information submitted under subsection (a).

''(c) CERTIFICATION.—The Administrator may require a representative of an independent assessment service to certify the accuracy and completeness of any information submitted under this section.

"§ 3613. Roles and responsibilities of agencies

''(a) IN GENERAL.—In implementing the requirements of FedRAMP, the head of each agency shall, consistent with guidance issued by the Director pursuant to section 3614—

''(1) promote the use of cloud computing products and services that meet FedRAMP security requirements and other risk-based performance requirements as determined by the Director, in consultation with the Secretary;

''(2) confirm whether there is a FedRAMP authorization in the secure mechanism provided under section 3609(a)(8) before beginning the process of granting a FedRAMP authorization for a cloud computing product or service;

''(3) to the extent practicable, for any cloud computing product or service the agency seeks to authorize that has received a FedRAMP authorization, use the existing assessments of security controls and materials within any FedRAMP authorization package for that cloud computing product or service; and

''(4) provide to the Director data and information required by the Director pursuant to section 3614 to determine how agencies are meeting metrics established by the Administrator.

''(b) ATTESTATION.—Upon completing an assessment or authorization activity with respect to a particular cloud computing product or service, if an agency determines that the information and data the agency has reviewed under paragraph (2) or (3) of subsection (a) is

wholly or substantially deficient for the purposes of performing an authorization of the cloud computing product or service, the head of the agency shall document as part of the resulting FedRAMP authorization package the reasons for this determination.

''(c) SUBMISSION OF AUTHORIZATIONS TO OPERATE REQUIRED.—Upon issuance of an agency authorization to operate based on a FedRAMP authorization, the head of the agency shall provide a copy of its authorization to operate letter and any supplementary information required pursuant to section 3609(a) to the Administrator.

''(d) SUBMISSION OF POLICIES REQUIRED.—Not later than 180 days after the date on which the Director issues guidance in accordance with section 3614(1), the head of each agency, acting through the chief information officer of the agency, shall submit to the Director all agency policies relating to the authorization of cloud computing products and services.

''(e) PRESUMPTION OF ADEQUACY.—

''(1) IN GENERAL.—The assessment of security controls and materials within the authorization package for a FedRAMP authorization shall be presumed adequate for use in an agency authorization to operate cloud computing products and services.

''(2) INFORMATION SECURITY REQUIREMENTS.—The presumption under paragraph (1) does not modify or alter—

''(A) the responsibility of any agency to ensure compliance with subchapter II of chapter 35 for any cloud computing product or service used by the agency; or

''(B) the authority of the head of any agency to make a determination that there is a demonstrable need for additional security requirements beyond the security requirements included in a FedRAMP authorization for a particular control implementation.

''§ 3614. Roles and responsibilities of the Office of Management and Budget

''The Director shall—

''(1) in consultation with the Administrator and the Secretary, issue guidance that—

''(A) specifies the categories or characteristics of cloud computing products and services that are within the scope of FedRAMP;

''(B) includes requirements for agencies to obtain a FedRAMP authorization when operating a cloud computing product or service de-

scribed in subparagraph (A) as a Federal information system; and

''(C) encompasses, to the greatest extent practicable, all necessary and appropriate cloud computing products and services;

''(2) issue guidance describing additional responsibilities of FedRAMP and the FedRAMP Board to accelerate the adoption of secure cloud computing products and services by the Federal Government;

''(3) in consultation with the Administrator, establish a process to periodically review FedRAMP authorization packages to support the secure authorization and reuse of secure cloud products and services;

''(4) oversee the effectiveness of FedRAMP and the FedRAMP Board, including the compliance by the FedRAMP Board with the duties described in section 3610(d); and

''(5) to the greatest extent practicable, encourage and promote consistency of the assessment, authorization, adoption, and use of secure cloud computing products and services within and across agencies.

"§ 3615. Reports to Congress; GAO report

''(a) REPORTS TO CONGRESS.—Not later than 1 year after the date of enactment of this section, and annually thereafter, the Director shall submit to the appropriate congressional committees a report that includes the following:

''(1) During the preceding year, the status, efficiency, and effectiveness of the General Services Administration under section 3609 and agencies under section 3613 and in supporting the speed, effectiveness, sharing, reuse, and security of authorizations to operate for secure cloud computing products and services.

''(2) Progress towards meeting the metrics required under section 3609(d).

''(3) Data on FedRAMP authorizations.

''(4) The average length of time to issue FedRAMP authorizations.

''(5) The number of FedRAMP authorizations submitted, issued, and denied for the preceding year.

''(6) A review of progress made during the preceding year in advancing automation techniques to securely automate FedRAMP processes and to accelerate reporting under this section.

''(7) The number and characteristics of authorized cloud computing products and services in use at

each agency consistent with guidance provided by the Director under section 3614.

''(8) A review of FedRAMP measures to ensure the security of data stored or processed by cloud service providers, which may include—

''(A) geolocation restrictions for provided products or services;

''(B) disclosures of foreign elements of supply chains of acquired products or services;

''(C) continued disclosures of ownership of cloud service providers by foreign entities; and

''(D) encryption for data processed, stored, or transmitted by cloud service providers.

''(b) GAO REPORT.—Not later than 180 days after the date of enactment of this section, the Comptroller General of the United States shall report to the appropriate congressional committees an assessment of the following:

''(1) The costs incurred by agencies and cloud service providers relating to the issuance of FedRAMP authorizations.

''(2) The extent to which agencies have processes in place to continuously monitor the implementation of cloud computing products and services operating as Federal information systems.

''(3) How often and for which categories of products and services agencies use FedRAMP authorizations.

''(4) The unique costs and potential burdens incurred by cloud computing companies that are small business concerns (as defined in section 3(a) of the Small Business Act (15 U.S.C. 632(a)) as a part of the FedRAMP authorization process.

''§ 3616. Federal Secure Cloud Advisory Committee

''(a) ESTABLISHMENT, PURPOSES, AND DUTIES.—

''(1) ESTABLISHMENT.—There is established a Federal Secure Cloud Advisory Committee (referred to in this section as the 'Committee') to ensure effective and ongoing coordination of agency adoption, use, authorization, monitoring, acquisition, and security of cloud computing products and services to enable agency mission and administrative priorities.

''(2) PURPOSES.—The purposes of the Committee are the following:

''(A) To examine the operations of FedRAMP and determine ways that authorization processes can continuously be improved, including the following:

''(i) Measures to increase agency reuse of FedRAMP authorizations.

"(ii) Proposed actions that can be adopted to reduce the burden, confusion, and cost associated with FedRAMP authorizations for cloud service providers.

"(iii) Measures to increase the number of FedRAMP authorizations for cloud computing products and services offered by small businesses concerns (as defined by section 3(a) of the Small Business Act (15 U.S.C. 632(a)).

"(iv) Proposed actions that can be adopted to reduce the burden and cost of FedRAMP authorizations for agencies.

"(B) Collect information and feedback on agency compliance with and implementation of FedRAMP requirements.

"(C) Serve as a forum that facilitates communication and collaboration among the FedRAMP stakeholder community.

"(3) DUTIES.—The duties of the Committee include providing advice and recommendations to the Administrator, the FedRAMP Board, and agencies on technical, financial, programmatic, and operational matters regarding secure adoption of cloud computing products and services.

''(b) MEMBERS.—

''(1) COMPOSITION.—The Committee shall be comprised of not more than 15 members who are qualified representatives from the public and private sectors, appointed by the Administrator, in consultation with the Director, as follows:

''(A) The Administrator or the Administrator's designee, who shall be the Chair of the Committee.

''(B) At least 1 representative each from the Cybersecurity and Infrastructure Security Agency and the National Institute of Standards and Technology.

''(C) At least 2 officials who serve as the Chief Information Security Officer within an agency, who shall be required to maintain such a position throughout the duration of their service on the Committee.

''(D) At least 1 official serving as Chief Procurement Officer (or equivalent) in an agency, who shall be required to maintain such a position throughout the duration of their service on the Committee.

''(E) At least 1 individual representing an independent assessment service.

"(F) At least 5 representatives from unique businesses that primarily provide cloud computing services or products, including at least 2 representatives from a small business concern (as defined by section 3(a) of the Small Business Act (15 U.S.C. 632(a))).

"(G) At least 2 other representatives of the Federal Government as the Administrator determines necessary to provide sufficient balance, insights, or expertise to the Committee.

"(2) DEADLINE FOR APPOINTMENT.—Each member of the Committee shall be appointed not later than 90 days after the date of enactment of this section.

"(3) PERIOD OF APPOINTMENT; VACANCIES.—

"(A) IN GENERAL.—Each non-Federal member of the Committee shall be appointed for a term of 3 years, except that the initial terms for members may be staggered 1-, 2-, or 3-year terms to establish a rotation in which one-third of the members are selected each year. Any such member may be appointed for not more than 2 consecutive terms.

"(B) VACANCIES.—Any vacancy in the Committee shall not affect its powers, but shall

be filled in the same manner in which the original appointment was made. Any member appointed to fill a vacancy occurring before the expiration of the term for which the member's predecessor was appointed shall be appointed only for the remainder of that term. A member may serve after the expiration of that member's term until a successor has taken office.

''(c) MEETINGS AND RULES OF PROCEDURES.—

''(1) MEETINGS.—The Committee shall hold not fewer than 3 meetings in a calendar year, at such time and place as determined by the Chair.

''(2) INITIAL MEETING.—Not later than 120 days after the date of enactment of this section, the Committee shall meet and begin the operations of the Committee.

''(3) RULES OF PROCEDURE.—The Committee may establish rules for the conduct of the business of the Committee if such rules are not inconsistent with this section or other applicable law.

''(d) EMPLOYEE STATUS.—

''(1) IN GENERAL.—A member of the Committee (other than a member who is appointed to the Committee in connection with another Federal appointment) shall not be considered an employee of

the Federal Government by reason of any service as such a member, except for the purposes of section 5703 of title 5, relating to travel expenses.

''(2) PAY NOT PERMITTED.—A member of the Committee covered by paragraph (1) may not receive pay by reason of service on the Committee.

''(e) APPLICABILITY TO THE FEDERAL ADVISORY COMMITTEE ACT.—Section 14 of the Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Committee.

''(f) DETAIL OF EMPLOYEES.—Any Federal Government employee may be detailed to the Committee without reimbursement from the Committee, and such detailee shall retain the rights, status, and privileges of his or her regular employment without interruption.

''(g) POSTAL SERVICES.—The Committee may use the United States mails in the same manner and under the same conditions as agencies.

''(h) REPORTS.—

''(1) INTERIM REPORTS.—The Committee may submit to the Administrator and Congress interim reports containing such findings, conclusions, and recommendations as have been agreed to by the Committee.

''(2) ANNUAL REPORTS.—Not later than 540 days after the date of enactment of this section, and annually thereafter, the Committee shall submit to the Administrator and Congress a report containing such findings, conclusions, and recommendations as have been agreed to by the Committee.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 36 of title 44, United States Code, is amended by adding at the end the following new items:

''3607. Definitions.
''3608. Federal Risk and Authorization Management Program.
''3609. Roles and responsibilities of the General Services Administration.
''3610. FedRAMP Board.
''3611. Independent assessment.
''3612. Declaration of foreign interests.
''3613. Roles and responsibilities of agencies.
''3614. Roles and responsibilities of the Office of Management and Budget.
''3615. Reports to Congress; GAO report.
''3616. Federal Secure Cloud Advisory Committee.''.

(c) SUNSET.—

(1) IN GENERAL.—Effective on the date that is 5 years after the date of enactment of this Act, chapter 36 of title 44, United States Code, is amended by striking sections 3607 through 3616.

(2) CONFORMING AMENDMENT.—Effective on the date that is 5 years after the date of enactment of this Act, the table of sections for chapter 36 of title 44, United States Code, is amended by striking the items relating to sections 3607 through 3616.

(d) RULE OF CONSTRUCTION.—Nothing in this section or any amendment made by this section shall be construed as altering or impairing the authorities of the Director of the Office of Management and Budget or the Secretary of Homeland Security under subchapter II of chapter 35 of title 44, United States Code.

Calendar No. 265

117TH CONGRESS
2D SESSION

S. 3600

A BILL

To improve the cybersecurity of the Federal Government, and for other purposes.

FEBRUARY 9, 2022

Read the second time and placed on the calendar