child sexual exploitation or preventing the online sexual exploitation of children.

''(6) METHOD OF PRESERVATION.—Not later than 1 year after the date of enactment of this paragraph, a provider of a report to the CyberTipline under subsection (a)(1) shall preserve materials under this subsection in a manner that is consistent with the most recent version of the Cybersecurity Framework developed by the National Institute of Standards and Technology, or any successor thereto.''.

SEC. 1094. STRENGTHENING OF DUTY TO REPORT APPARENT VIOLATIONS TO CYBERTIPLINE RELATED TO ONLINE EXPLOITATION OF CHILDREN.

(a) AMENDMENTS.—Section 2258A of title 18, United States Code, is amended—

(1) in subsection (a)(2)(A), by inserting '', of section 1591 (if the violation involves a minor), or of 2422(b)'' after ''child pornography''; and

(2) in subsection (e)—

(A) in paragraph (1), by striking ''$150,000'' and inserting ''$850,000 in the case of a provider with not less than 100,000,000 monthly active users or $600,000 in the case of a provider with less than 100,000,000 monthly active users''; and

(B) in paragraph (2), by striking ''$300,000'' and inserting ''$1,000,000 in the case of a provider with not less than 100,000,000 monthly active users or $850,000 in the case of a provider with less than 100,000,000 monthly active users''.

(b) GUIDELINES.—Not later than 180 days after the date of enactment of this Act, the National Center for Missing & Exploited Children may issue guidelines, as appropriate, to providers required or permitted to take actions described in section 2258A(a)(1)(B) of title 18, United States Code, on the relevant identifiers for content that may indicate sex trafficking of children, as described in section 1591 of that title, or enticement, as described in section 2422(b) of that title.

SA 796. Mr. SCHUMER submitted an amendment intended to be proposed by him to the bill S. 2226, to authorize appropriations for fiscal year 2024 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end, the following:

DIVISION F—COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

TITLE LX—FEDERAL INFORMATION SECURITY AND MODERNIZATION ACT OF 2023

SECTION 6001. SHORT TITLE.

(a) SHORT TITLE.—This title may be cited as the ''Federal Information Security Modernization Act of 2023''.

SEC. 6002. DEFINITIONS.

In this title, unless otherwise specified:

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

(2) 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 Accountability of the House of Representatives; and

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

(3) AWARDEE.—The term ''awardee'' has the meaning given the term in section 3591 of title 44, United States Code, as added by this title.

(4) CONTRACTOR.—The term ''contractor'' has the meaning given the term in section 3591 of title 44, United States Code, as added by this title.

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

(6) FEDERAL INFORMATION SYSTEM.—The term ''Federal information system'' has the meaning give the term in section 3591 of title 44, United States Code, as added by this title.

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

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

(9) 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.

(10) THREAT HUNTING.—The term ''threat hunting'' means proactively and iteratively searching systems for threats and vulnerabilities, including threats or vulnerabilities that may evade detection by automated threat detection systems.

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

SEC. 6003. AMENDMENTS TO TITLE 44.

(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) privacy, confidentiality, 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)—

(i) by redesignating paragraph (2) as paragraph (3); and

(ii) 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 of information collected or maintained by or for agencies;

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

(2) 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 information 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 consult, 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,'';

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

(D) by adding at the end the following:

''(j)(1) Nothwithstanding paragraphs (2) and (3) of subsection (a), the head of each agency shall designate a Chief Privacy Officer with the necessary skills, knowledge, and expertise, who shall have the authority and responsibility to—

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

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

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

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

''(B) have visibility into relevant agency operations; and

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

''(3) A privacy officer of an agency established under a statute enacted before the date of enactment of the Federal Information Security Modernization Act of 2023 may carry out the responsibilities under this subsection for the agency.''; 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 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 (2), (3), (4), (5), (6), and (7) as paragraphs (3), (4), (5), (6), (8), and (10), respectively;

(B) by inserting after paragraph (1) the following:

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

(C) by inserting after paragraph (6), as so redesignated, the following:

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

(D) in paragraph (8)(A), as so redesignated, by striking ''used'' and inserting ''owned, managed,'';

(E) by inserting after paragraph (8), as so redesignated, the following:

''(9) 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 (10), as so redesignated, the following:

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

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

(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(c)(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)(8)(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)(8)(A)(i)''.

(D) INTERNET OF THINGS CYBERSECURITY IMPROVEMENT ACT OF 2020.—Section 3(5) of the Internet of Things Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3a(5)) 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 semicolon; 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 (5), by striking ''and'' at the end;

(ii) in paragraph (6), by striking the period at the end and inserting ''; and''; and

(iii) by adding at the end the following:

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

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

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

(B) in subsection (b)—

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

(ii) in paragraph (2)(A), by inserting ''and reporting requirements under subchapter IV of this chapter'' after ''section 3556'';

(iii) by redesignating paragraphs (8) and (9) as paragraphs (10) and (11), respectively; and

(iv) by inserting after paragraph (7) the following:

''(8) expeditiously seeking opportunities to reduce costs, administrative burdens, and other barriers to information technology security and modernization for agencies, including through shared services for cybersecurity capabilities identified as appropriate by the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and other agencies as appropriate;'';

(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)'';

(II) by inserting '', which shall be unclassified but may include 1 or more annexes that contain classified or other sensitive information, as appropriate'' after ''a report''; and

(III) 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; and

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

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

(D) in subsection (h)—

(i) in paragraph (2)—

(I) in subparagraph (A), by inserting ''and the National Cyber Director'' after ''in coordination with the Director''; and

(II) in subparagraph (D), by inserting '', the National Cyber Director,'' after ''notify the Director''; and

(ii) in paragraph (3)(A)(iv), by inserting '', the National Cyber Director,'' after ''the Secretary provides prior notice to the Director'';

(E) by amending subsection (i) to read as follows:

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

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

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

''(3) analysis of incident information under section 3597;

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

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

''(6) evaluation of agency threat hunting results;

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

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

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

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

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

(F) by adding at the end the following:

''(m) DIRECTIVES.—

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

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

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

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

''(2) BINDING OPERATIONAL DIRECTIVE UPDATES.—If the Secretary issues a binding operational directive under this section, the Director of the Cybersecurity and Infrastructure Security Agency shall submit to the Director, the National Cyber Director, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committees on Oversight and Accountability

and Homeland Security of the House of Representatives an update on the status of the implementation of the binding operational directive at agencies not later than 30 days after the issuance of the binding operational directive, and every 90 days thereafter until—

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

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

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

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

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

''(B) has not implemented a binding operational directive.

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

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

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

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

''(o) AUTOMATED STANDARD IMPLEMENTATION VERIFICATION.—When the Director of the National Institute of Standards and Technology issues a proposed standard or guideline pursuant to paragraphs (2) or (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)), the Director of the National Institute of Standards and Technology shall consider developing and, if appropriate and practical, develop specifications to enable the automated verification of the implementation of the controls.

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

(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, assessing agency system risk, as applicable, by—

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

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

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

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

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

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

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

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

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

''(IV) incidents; and

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

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

''(viii) assessing the consequences of potential incidents occurring on agency systems that would impact systems at other agencies, including due to interconnectivity between different agency systems or operational reliance on the operations of the system or data in the system;'';

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

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

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

''(I) the Director;

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

''(III) the National Cyber Director;'';

(ii) in paragraph (2)—

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

(II) in subparagraph (D), by inserting '', through the use of penetration testing, the vulnerability disclosure program established under section 3559B, and other means,'' after ''periodically'';

(iii) in paragraph (3)(A)—

(I) in the matter preceding clause (i), by striking ''senior agency information security officer'' and inserting ''Chief Information Security Officer'';

(II) in clause (i), by striking ''this section'' and inserting ''subsections (a) through (c)'';

(III) in clause (ii), by striking ''training and'' and inserting ''skills, training, and'';

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

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

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

(VI) in clause (iv), as so redesignated, by striking ''information security duties as that official's primary duty'' and inserting ''information, computer network, and technology security duties as the Chief Information Security Officers' primary duty'';

(iv) in paragraph (5), by striking ''annually'' and inserting ''not less frequently than quarterly''; and

(v) in paragraph (6), by striking ''official delegated'' and inserting ''Chief Information Security Officer delegated''; and

(B) in subsection (b)—

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

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

(ii) in paragraph (2)—

(I) by striking subparagraph (B);

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

(III) in subparagraph (B), as so redesignated, by striking ''and'' at the end; and

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

(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 issued by the Secretary 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 the agency risk assessment required under subsection (a)(1)(A);

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

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

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

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

(vi) 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 (II), by adding ''and'' at the end;

(bb) by striking subclause (III); and

(cc) by redesignating subclause (IV) as subclause (III); and

(C) in subsection (c)—

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

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

''(1) BIENNIAL REPORT.—Not later than 2 years after the date of enactment of the Federal Information Security Modernization Act of 2023 and not less frequently than once every 2 years thereafter, using the continuous and ongoing agency system risk assessment required under subsection (a)(1)(A), the head of each agency shall submit to the Director, the National Cyber Director, the Director of the Cybersecurity and Infrastructure Security Agency, the Comptroller General of the United States, the majority and minority leaders of the Senate, the Speaker and minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Accountability of the House of Representatives, the Committee on Homeland Security of the House of Representatives, the Committee on Commerce, Science, and Transportation of the Senate, the Committee on Science, Space, and Technology of the House of Representatives, and the appropriate authorization and appropriations committees of Congress a report that—

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

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

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

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

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

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

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

(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 performing, or reviewing the results of, agency 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) 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

(F) 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;

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

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

''(D) any other element the Director determines appropriate.''; 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 Commerce, Science, and Transportation of the Senate;

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

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

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

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

''(I) the Director;

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

''(K) the National Cyber Director;

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

''(M) the inspector general of any impacted agency.

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

''(A) means—

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

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

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

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

''(3) BREACH.—The term 'breach'—

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

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

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

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

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

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

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

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

"§ 3592. Notification of breach

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

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

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

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

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

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

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

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

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

''(C) the type of breach; and

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

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

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

''(B) through an appropriate alternative method of notification.

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

''(1) a brief description of the breach;

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

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

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

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

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

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

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

''(d) DELAY OF NOTIFICATION.—

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

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

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

''(C) reveal sensitive sources and methods;

''(D) cause damage to national security; or

''(E) hamper security remediation actions.

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

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

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

''(f) DELAY OF NOTIFICATION REPORT.—

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

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

''(g) CONGRESSIONAL REPORTING REQUIREMENTS.—

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

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

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

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

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

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

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

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

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

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

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

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

''(C) the appropriations committees of Congress;

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

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

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

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

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

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

''(1) limit—

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

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

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

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

''(i) the Director;

''(ii) the National Cyber Director;

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

''(iv) any other agency;

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

''(i) breaches that are not covered breaches; and

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

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

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

"§ 3593. Congressional and Executive Branch reports on major incidents

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

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

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

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

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

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

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

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

''(8) the appropriate authorization and appropriations committees of Congress

''(b) INITIAL NOTIFICATION.—

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

''(2) CONTENTS.—A notification required under paragraph (1) with respect to a major

incident shall include the following, based on information available to agency officials as of the date on which the agency submits the notification:

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

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

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

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

''(C) A preliminary assessment of the impacts to—

''(i) the agency;

''(ii) the Federal Government;

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

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

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

''(c) SUPPLEMENTAL UPDATE.—Within a reasonable amount of time, but not later than 30 days after the date on which the head of an agency submits a written notification under subsection (a), the head of the agency shall provide to the appropriate congressional entities an unclassified and written update, which may include 1 or more annexes that contain classified or other sensitive information, as appropriate, on the major incident, based on information available to agency officials as of the date on which the agency provides the update, on—

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

''(A) the agency;

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

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

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

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

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

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

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

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

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

''(f) REPORT DELIVERY.—

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

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

''(B) may be submitted in a paper format.

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

''(A) shall be—

''(i) unclassified; and

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

''(B) may include classified annexes, as appropriate.

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

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

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

''(A) include, at a minimum—

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

''(ii) the identity of the reporting agency; and

''(iii) the date of submission; and

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

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

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

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

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

''(3) the appropriations committees of Congress;

''(4) the appropriate authorization committees of Congress;

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

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

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

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

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

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

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

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

''(1) limit—

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

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

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

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

''§ 3594. Government information sharing and incident response

''(a) IN GENERAL.—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

''(I) impacted by the incident;

''(II) particularly susceptible to the incident; or

''(III) similarly targeted by the incident; and

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

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

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

''(4) NATIONAL SECURITY SYSTEMS EXEMPTION.—

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

''(B) PROTECTIONS.—Any information sharing and handling of information under this paragraph shall be appropriately protected consistent with procedures authorized for the protection of sensitive sources and methods or by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

''(b) AUTOMATION.—In providing information and selecting a method to provide information under subsection (a), the head of each agency shall implement subsection (a)(1) in a manner that provides such information to the Cybersecurity and Infrastructure Security Agency in an automated and machine-readable format, to the greatest extent practicable.

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

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

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

''§ 3595. Responsibilities of contractors and awardees

''(a) REPORTING.—

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

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

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

''(C) a component of any Federal information system operated, managed, or maintained by a contractor or awardee contains a security vulnerability, including a supply chain compromise or an identified software or hardware vulnerability, for which there is reliable evidence of attempted or successful exploitation of the vulnerability by an actor without authorization of the Federal information system owner; or

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

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

''(3) PROCEDURES.—

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

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

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

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

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

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

''(4) GUIDANCE.—The Director shall issue guidance to agencies relating to the scope of vulnerabilities to be reported under paragraph (2), such as the minimum severity of a vulnerability required to be reported or whether vulnerabilities that are already publicly disclosed must be reported.

''(b) REGULATIONS; MODIFICATIONS.—

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

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

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

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

''(3) CONGRESSIONAL NOTIFICATION.—

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

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

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

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

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

''§ 3596. Training

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

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

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

''(b) BEST PRACTICES AND CONSISTENCY.—The Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director, the National Cyber Director, and the Director of the National Institute of Standards and Technology, shall develop best practices to support consistency across agencies in cybersecurity incident response training, including—

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

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

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

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

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

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

''§ 3597. Analysis and report on Federal incidents

''(a) ANALYSIS OF FEDERAL INCIDENTS.—

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

''(A) the causes of incidents, including—

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

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

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

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

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

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

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

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

''(3) SHARING OF DATA AND ANALYSIS.—

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

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

''(ii) support the cybersecurity improvement efforts of agencies.

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

''(i) in human-readable written products; and

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

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

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

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

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

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

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

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

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

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

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

''(c) PUBLICATION.—

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

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

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

''(4) REQUIREMENT FOR COMPILING INFORMATION.—

''(A) COMPILATION.—Subject to subparagraph (B), in making a report publicly available under paragraph (1), the Director of the Cybersecurity and Infrastructure Security Agency shall sufficiently compile information so that no specific incident of an agency can be identified.

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

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

''(ii) in consultation with the impacted agency; and

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

''(d) INFORMATION PROVIDED BY AGENCIES.—

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

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

''(e) NATIONAL SECURITY SYSTEM REPORTS.—

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

''(A) the majority and minority leaders of the Senate,

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

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

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

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

''(F) the Committee on Appropriations of the Senate;

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

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

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

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

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

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

''§ 3598. Major incident definition

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

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

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

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

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

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

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

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

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

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

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

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

''(B) is enabled by—

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

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

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

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

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

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

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

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

(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

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

SEC. 6004. 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, as appropriate—

''(i) a cybersecurity risk management plan; and

''(ii) a supply chain risk assessment in accordance with section 1326 of title 41.''; 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,''; and

(B) in subsection (h), by inserting '', including cybersecurity performances,'' after ''the performances''; and

(2) in section 11303(b)(2)(B)—

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

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

(C) by adding at the end the following:

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

(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 11317, by inserting ''security,'' before ''or schedule''; and

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

SEC. 6005. 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) UPDATING FISMA 2014.—Section 2 of the Federal Information Security Modernization Act of 2014 (Public Law 113–283; 128 Stat. 3073) is amended—

(A) by striking subsections (b) and (d); and

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

(2) INCIDENT DATA SHARING.—

(A) IN GENERAL.—The Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall develop, and as appropriate update, guidance, 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) 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; and

(ii) include requirements for the timeliness of data production.

(C) AUTOMATION.—The Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall promote, as feasible, the use of automation and machine-readable data for data sharing under section 3594(a) of title 44, United States Code, as added by this title.

(3) CONTRACTOR AND AWARDEE GUIDANCE.—

(A) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Director shall issue guidance to 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 agencies of incidents involving information of the Federal Government.

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

SEC. 6006. ADDITIONAL GUIDANCE TO AGENCIES ON FISMA UPDATES.

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

(2) establishing a process for securely providing the status of each remedial action for high value assets under section 3554(b)(7) of title 44, United States Code, as amended by this Act, to the Director and the Director of 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.

(b) COORDINATION.—The head of each agency shall coordinate with the inspector general of the agency, as applicable, to ensure consistent understanding of agency policies for the purpose of evaluations conducted by the inspector general.

SEC. 6007. 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 1 year after the date of enactment of this Act, the Director shall develop, in consultation with the National Cyber Director, and issue guidance requiring the head of each agency to notify a reporting entity, and take into consideration the need to coordinate with Sector Risk Management Agencies (as defined in

section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650)), as appropriate, of an incident at the agency 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) any information system (as defined in section 3502 of title 44, United States Code) used in the transmission or storage of the sensitive information described in paragraph (1).

SEC. 6008. MOBILE SECURITY BRIEFINGS.

(a) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Director shall provide to the appropriate congressional committees—

(1) a briefing on the compliance of agencies with the No TikTok on Government Devices Act (44 U.S.C. 3553 note; Public Law 117–328); and

(2) as a component of the briefing required under paragraph (1), a list of each exception of an agency from the No TikTok on Government Devices Act (44 U.S.C. 3553 note; Public Law 117–328), which may include a classified annex.

(b) ADDITIONAL BRIEFING.—Not later than 1 year after the date of the briefing required under subsection (a)(1), the Director shall provide to the appropriate congressional committees—

(1) a briefing on the compliance of any agency that was not compliant with the No TikTok on Government Devices Act (44 U.S.C. 3553 note; Public Law 117–328) at the time of the briefing required under subsection (a)(1); and

(2) as a component of the briefing required under paragraph (1), an update to the list required under subsection (a)(2).

SEC. 6009. DATA AND LOGGING RETENTION FOR INCIDENT RESPONSE.

(a) GUIDANCE.—Not later than 2 years after the date of enactment of this Act, the Director, in consultation with the National Cyber Director and the Director of the Cybersecurity and Infrastructure Security Agency, shall 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.

(b) NATIONAL SECURITY SYSTEMS.—The Secretary of Defense shall issue guidance that meets or exceeds the standards required in guidance issued under subsection (a) for National Security Systems.

SEC. 6010. CISA AGENCY LIAISONS.

(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 liaison to the Chief Information Security Officer of each agency.

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

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

(2) risk assessments of agency systems; and

(3) other Federal cybersecurity initiatives.

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

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

(2) supporting, as requested, incident response coordination between the assigned agency and the Cybersecurity and Infrastructure Security Agency;

(3) becoming familiar with assigned agency systems, processes, and procedures to better facilitate support to the agency; and

(4) other liaison duties to the assigned agency solely in furtherance of Federal cybersecurity or support to the assigned agency as a Sector Risk Management Agency, as assigned by the Director of the Cybersecurity and Infrastructure Security Agency in consultation with the head of the assigned agency.

(d) LIMITATION.—A liaison assigned under subsection (a) shall not be a contractor.

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

(f) COORDINATION OF ACTIVITIES.—The Director of the Cybersecurity and Infrastructure Security Agency shall consult with the Director on the execution of the duties of the Cybersecurity and Infrastructure Security Agency liaisons to ensure that there is no inappropriate duplication of activities among—

(1) Federal cybersecurity support to agencies of the Office of Management and Budget; and

(2) the Cybersecurity and Infrastructure Security Agency liaison.

(g) RULE OF CONSTRUCTION.—Nothing in this section shall be construed impact the ability of the Director to support agency implementation of Federal cybersecurity requirements pursuant to subchapter II of chapter 35 of title 44, United States Code, as amended by this Act.

SEC. 6011. 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) GUIDANCE.—The Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, shall issue guidance to agencies that—

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

''(2) provides policies governing the development of—

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

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

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

''(4) in no manner restricts the authority of the Secretary of Homeland Security or the Director of the Cybersecurity and Infrastructure Agency to conduct threat hunting pursuant to section 3553 of title 44, United States Code, or penetration testing under this chapter.

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

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

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

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

(b) EXISTING GUIDANCE.—

(1) IN GENERAL.—Compliance with guidance issued by the Director relating to penetration testing before the date of enactment of this Act shall be deemed to be compliance with section 3559A of title 44, United States Code, as added by this title.

(2) IMMEDIATE NEW GUIDANCE NOT REQUIRED.—Nothing in section 3559A of title 44, United States Code, as added by this title, shall be construed to require the Director to issue new guidance to agencies relating to penetration testing before the date described in paragraph (3).

(3) GUIDANCE UPDATES.—Notwithstanding paragraphs (1) and (2), not later than 2 years after the date of enactment of this Act, the Director shall review and, as appropriate, update existing guidance requiring penetration testing by agencies.

(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) PENETRATION TESTING BY THE SECRETARY OF HOMELAND SECURITY.—Section 3553(b) of title 44, United States Code, as amended by this title, is further amended by inserting after paragraph (8) the following:

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

''(A) without consent or authorization from agencies; and

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

SEC. 6012. VULNERABILITY DISCLOSURE POLICIES.

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

"§ 3559B. Federal vulnerability disclosure policies

''(a) PURPOSE; SENSE OF CONGRESS.—

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

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

''(b) DEFINITIONS.—In this section:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

''(f) RESPONSIBILITIES OF AGENCIES.—

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

''(A) an appropriate security contact; and

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

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

''(A) describe—

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

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

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

''(iv) the disclosure policy for a contractor; and

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

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

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

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

''(C) include any other relevant information; and

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

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

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

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

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

''(g) EXEMPTIONS.—

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

''(2) LIMITATION.—The Director and the head of each agency may not publish under subsection (f)(1) or include in a vulnerability disclosure policy under subsection (f)(2) host names, services, information systems, or other information that the Director or the head of an agency, in coordination with the Director and other appropriate heads of agencies, determines would—

''(A) disrupt a law enforcement investigation;

''(B) endanger national security or intelligence activities; or

''(C) impede national defense activities or military operations.

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

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

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

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

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

(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 this title, the following:

''3559B. Federal vulnerability disclosure policies.''.

(c) CONFORMING UPDATE AND REPEAL.—

(1) GUIDELINES ON THE DISCLOSURE PROCESS FOR SECURITY VULNERABILITIES RELATING TO INFORMATION SYSTEMS, INCLUDING INTERNET OF THINGS DEVICES.—Section 5 of the IoT Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3c) is amended by striking subsections (d) and (e).

(2) IMPLEMENTATION AND CONTRACTOR COMPLIANCE.—The IoT Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3a et seq.) is amended—

(A) by striking section 6 (15 U.S.C. 278g–3d); and

(B) by striking section 7 (15 U.S.C. 278g–3e).

SEC. 6013. IMPLEMENTING ZERO TRUST ARCHITECTURE.

(a) BRIEFINGS.—Not later than 1 year after the date of enactment of this Act, the Director shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committees on Oversight and Accountability and Homeland Security of the House of Representatives a briefing 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, including through the transition to zero trust architecture;

(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; and

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

(b) PROGRESS REPORT.—As a part of each report required to be submitted under section 3553(c) of title 44, United States Code, during the period beginning on the date that is 4 years after the date of enactment of this Act and ending on the date that is 10 years after the date of enactment of this Act, the Director shall include an update on agency implementation of zero trust architecture, which shall include—

(1) a description of steps agencies have completed, including progress toward achieving any 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.

(c) CLASSIFIED ANNEX.—Each update required under subsection (b) may include 1 or more annexes that contain classified or other sensitive information, as appropriate.

(d) NATIONAL SECURITY SYSTEMS.—

(1) BRIEFING.—Not later than 1 year after the date of enactment of this Act, the Secretary of Defense shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Accountability of the House of Representatives, the Committee on Armed Services of the Senate, the Committee on Armed Services of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives a briefing on the implementation of zero trust architecture with respect to national security systems.

(2) PROGRESS REPORT.—Not later than the date on which each update is required to be submitted under subsection (b), the Secretary of Defense shall submit to the congressional committees described in paragraph (1) a progress report on the implementation of zero trust architecture with respect to national security systems.

SEC. 6014. AUTOMATION AND ARTIFICIAL INTELLIGENCE.

(a) DEFINITION.—In this section, the term ''information system'' has the meaning given the term in section 3502 of title 44, United States Code.

(b) USE OF ARTIFICIAL INTELLIGENCE.—

(1) IN GENERAL.—As appropriate, the Director shall issue guidance on the use of artificial intelligence by agencies to improve the cybersecurity of information systems.

(2) CONSIDERATIONS.—The Director and head of each agency shall consider the use and capabilities of artificial intelligence systems wherever automation is used in furtherance of the cybersecurity of information systems.

(3) REPORT.—Not later than 1 year after the date of enactment of this Act, and annually thereafter until the date that is 5 years after the date of enactment of this Act, the Director shall submit to the appropriate congressional committees a report on the use of artificial intelligence to further the cybersecurity of information systems.

(c) COMPTROLLER GENERAL REPORTS.—

(1) IN GENERAL.—Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall submit to the appropriate congressional committees a report on the risks to the privacy of individuals and the cybersecurity of information systems associated with the use by Federal agencies of artificial intelligence systems or capabilities.

(2) STUDY.—Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall perform a study, and submit to the Committees on Homeland Security and Governmental Affairs and Commerce, Science, and Transportation of the Senate and the Committees on Oversight and Accountability, Homeland Security, and Science, Space, and Technology of the House of Representatives a report, on the use of automation, including artificial intelligence, and machine-readable data across the Federal Government for cybersecurity purposes, including the automated updating of cybersecurity tools, sensors, or processes employed by agencies under paragraphs (1), (5)(C), and (8)(B) of section 3554(b) of title 44, United States Code, as amended by this title.

SEC. 6015. 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 ''December 31, 2031''.

SEC. 6016. COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY DASHBOARD.

(a) DASHBOARD REQUIRED.—Section 424(e) of title 5, United States Code, is amended—

(1) in paragraph (2)—

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

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

(C) 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; and''; and

(2) by adding at the end the following:

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

SEC. 6017. SECURITY OPERATIONS CENTER SHARED SERVICE.

(a) BRIEFING.—Not later than 180 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 Accountability of the House of Representatives a briefing on—

(1) existing security operations center shared services;

(2) the capability for such shared service to offer centralized and simultaneous support to multiple agencies;

(3) the capability for such shared service to integrate with or support agency threat hunting activities authorized under section 3553 of title 44, United States Code, as amended by this title;

(4) the capability for such shared service to integrate with or support Federal vulnerability management activities; and

(5) future plans for expansion and maturation of such shared service.

(b) GAO REPORT.—Not less than 540 days after the date of enactment of this Act, the Comptroller General of the United States shall submit to the appropriate congressional committees a report on Federal cybersecurity security operations centers that—

(1) identifies Federal agency best practices for efficiency and effectiveness;

(2) identifies non-Federal best practices used by large entity operations centers and entities providing operation centers as a service; and

(3) includes recommendations for the Cybersecurity and Infrastructure Security Agency and any other relevant agency to improve the efficiency and effectiveness of security operations centers shared service offerings.

SEC. 6018. FEDERAL CYBERSECURITY REQUIREMENTS.

(a) CODIFYING FEDERAL CYBERSECURITY REQUIREMENTS IN TITLE 44.—

(1) AMENDMENT TO FEDERAL CYBERSECURITY ENHANCEMENT ACT OF 2015.—Section 225 of the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1523) is amended by striking subsections (b) and (c).

(2) TITLE 44.—Section 3554 of title 44, United States Code, as amended by this title, is further amended by adding at the end the following:

''(f) SPECIFIC CYBERSECURITY REQUIREMENTS AT AGENCIES.—

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

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

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

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

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

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

''(i) remote access to a information system; and

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

''(2) PROHIBITION.—

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

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

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

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

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

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

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

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

''(4) DURATION OF CERTIFICATION.—

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

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

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

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

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

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

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

''(g) EXCEPTION.—

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

''(A) the Department of Defense;

''(B) a national security system; or

''(C) an element of the intelligence community.

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

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

''(B) national security systems; or

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

''(i) necessary for research purposes; or

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

(b) REPORT ON EXEMPTIONS.—Section 3554(c)(1) of title 44, United States Code, as amended by this title, is further amended—

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

(2) in subparagraph (D), by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following:

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

(c) DURATION OF CERTIFICATION EFFECTIVE DATE.—Paragraph (3) of section 3554(f) of title 44, United States Code, as added by this title, shall take effect on the date that is 1 year after the date of enactment of this Act.

(d) FEDERAL CYBERSECURITY ENHANCEMENT ACT OF 2015 UPDATE.—Section 222(3)(B) of the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1521(3)(B)) is amended by inserting ''and the Committee on Oversight and Accountability'' before ''of the House of Representatives.''

SEC. 6019. FEDERAL CHIEF INFORMATION SECURITY OFFICER.

(a) AMENDMENT.—Chapter 36 of title 44, United States Code, is amended by adding at the end the following:

''§ 3617. Federal chief information security officer

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

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

''(2) the Office of the National Cyber Director.

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

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

''(1) every function under this chapter;

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

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

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

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

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

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

''(e) COORDINATION WITH ONCD.—The Federal Chief Information Security Officer shall support initiatives determined by the Federal Chief Information Officer necessary to coordinate with the Office of the National Cyber Director.''.

(b) NATIONAL CYBER DIRECTOR DUTIES.—Section 1752 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500) is amended—

(1) by redesignating subsection (g) as subsection (h); and

(2) by inserting after subsection (f) the following:

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

(c) TREATMENT OF INCUMBENT.—The individual serving as the Federal Chief Information Security Officer appointed by the President as of the date of the enactment of this Act may serve as the Federal Chief Information Security Officer under section 3617 of title 44, United States Code, as added by this title, beginning on the date of enactment of this Act, without need for a further or additional appointment under such section.

(d) CLERICAL AMENDMENT.—The table of sections for chapter 36 of title 44, United States Code, is amended by adding at the end the following:

''Sec. 3617. Federal chief information security officer''.

SEC. 6020. RENAMING OFFICE OF THE FEDERAL CHIEF INFORMATION OFFICER.

(a) DEFINITIONS.—

(1) IN GENERAL.—Section 3601 of title 44, United States Code, is amended—

(A) by striking paragraph (1); and

(B) by redesignating paragraphs (2) through (8) as paragraphs (1) through (7), respectively.

(2) CONFORMING AMENDMENTS.—

(A) TITLE 10.—Section 2222(i)(6) of title 10, United States Code, is amended by striking ''section 3601(4)'' and inserting ''section 3601''.

(B) NATIONAL SECURITY ACT OF 1947.—Section 506D(k)(1) of the National Security Act of 1947 (50 U.S.C. 3100(k)(1)) is amended by striking ''section 3601(4)'' and inserting ''section 3601''.

(b) OFFICE OF ELECTRONIC GOVERNMENT.—Section 3602 of title 44, United States Code, is amended—

(1) in the heading, by striking ''**OFFICE OF ELECTRONIC GOVERNMENT**'' and inserting ''**OFFICE OF THE FEDERAL CHIEF INFORMATION OFFICER**'';

(2) in subsection (a), by striking ''Office of Electronic Government'' and inserting ''Office of the Federal Chief Information Officer'';

(3) in subsection (b), by striking ''an Administrator'' and inserting ''a Federal Chief Information Officer'';

(4) in subsection (c), in the matter preceding paragraph (1), by striking ''The Administrator'' and inserting ''The Federal Chief Information Officer'';

(5) in subsection (d), in the matter preceding paragraph (1), by striking ''The Administrator'' and inserting ''The Federal Chief Information Officer'';

(6) in subsection (e), in the matter preceding paragraph (1), by striking ''The Administrator'' and inserting ''The Federal Chief Information Officer'';

(7) in subsection (f)—

(A) in the matter preceding paragraph (1), by striking ''the Administrator'' and inserting ''the Federal Chief Information Officer''; and

(B) in paragraph (16), by striking ''the Office of Electronic Government'' and inserting ''the Office of the Federal Chief Information Officer''; and

(8) in subsection (g), by striking ''the Office of Electronic Government'' and inserting ''the Office of the Federal Chief Information Officer''.

(c) CHIEF INFORMATION OFFICERS COUNCIL.—Section 3603 of title 44, United States Code, is amended—

(1) in subsection (b)(2), by striking ''The Administrator of the Office of Electronic Government'' and inserting ''The Federal Chief Information Officer'';

(2) in subsection (c)(1), by striking ''The Administrator of the Office of Electronic Government'' and inserting ''The Federal Chief Information Officer''; and

(3) in subsection (f)—

(A) in paragraph (3), by striking ''the Administrator'' and inserting ''the Federal Chief Information Officer''; and

(B) in paragraph (5), by striking ''the Administrator'' and inserting ''the Federal Chief Information Officer''.

(d) E-GOVERNMENT FUND.—Section 3604 of title 44, United States Code, is amended—

(1) in subsection (a)(2), by striking ''the Administrator of the Office of Electronic Government'' and inserting ''the Federal Chief Information Officer'';

(2) in subsection (b), by striking ''Administrator'' each place it appears and inserting ''Federal Chief Information Officer''; and

(3) in subsection (c), in the matter preceding paragraph (1), by striking ''the Administrator'' and inserting ''the Federal Chief Information Officer''.

(e) PROGRAM TO ENCOURAGE INNOVATIVE SOLUTIONS TO ENHANCE ELECTRONIC GOVERNMENT SERVICES AND PROCESSES.—Section 3605 of title 44, United States Code, is amended—

(1) in subsection (a), by striking ''The Administrator'' and inserting ''The Federal Chief Information Officer'';

(2) in subsection (b), by striking '', the Administrator,'' and inserting '', the Federal Chief Information Officer,''; and

(3) in subsection (c)—

(A) in paragraph (1)—

(i) by striking ''The Administrator'' and inserting ''The Federal Chief Information Officer''; and

(ii) by striking ''proposals submitted to the Administrator'' and inserting ''proposals submitted to the Federal Chief Information Officer'';

(B) in paragraph (2)(B), by striking ''the Administrator'' and inserting ''the Federal Chief Information Officer''; and

(C) in paragraph (4), by striking ''the Administrator'' and inserting ''the Federal Chief Information Officer''.

(f) E-GOVERNMENT REPORT.—Section 3606 of title 44, United States Code, is amended in the section heading by striking ''**E-Government**'' and inserting ''**Annual**''.

(g) TREATMENT OF INCUMBENT.—The individual serving as the Administrator of the Office of Electronic Government under section 3602 of title 44, United States Code, as of the date of the enactment of this Act, may continue to serve as the Federal Chief Information Officer commencing as of that date, without need for a further or additional appointment under such section.

(h) TECHNICAL AND CONFORMING AMENDMENTS.—The table of sections for chapter 36 of title 44, United States Code, is amended—

(1) by striking the item relating to section 3602 and inserting the following:

''3602. Office of the Federal Chief Information Officer.''; and

(2) in the item relating to section 3606, by striking ''E–Government'' and inserting ''Annual''.

(i) REFERENCES.—

(1) ADMINISTRATOR.—Any reference to the Administrator of the Office of Electronic Government in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Federal Chief Information Officer.

(2) OFFICE OF ELECTRONIC GOVERNMENT.—Any reference to the Office of Electronic Government in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Office of the Federal Chief Information Officer.

SEC. 6021. RULES OF CONSTRUCTION.

(a) AGENCY ACTIONS.—Nothing in this title, or an amendment made by this title, shall be construed to authorize the head of an agency to take an action that is not authorized by this title, an amendment made by this title, or existing law.

(b) PROTECTION OF RIGHTS.—Nothing in this title, or an amendment made by this title, shall be construed to permit the violation of the rights of any individual protected by the

Constitution of the United States, including through censorship of speech protected by the Constitution of the United States or unauthorized surveillance.

TITLE LXI—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Subtitle A—National Risk Management Cycle

SEC. 6101. SHORT TITLE.

This subtitle may be cited as the ''National Risk Management Act of 2023''.

SEC. 6102. NATIONAL RISK MANAGEMENT CYCLE.

(a) IN GENERAL.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended by adding at the end the following:

''SEC. 2220F. NATIONAL RISK MANAGEMENT CYCLE.

''(a) NATIONAL CRITICAL FUNCTIONS DEFINED.—In this section, the term 'national critical functions' means the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

''(b) NATIONAL RISK MANAGEMENT CYCLE.—

''(1) RISK IDENTIFICATION AND ASSESSMENT.—

''(A) IN GENERAL.—The Secretary, acting through the Director, shall establish a recurring process by which to identify and assess risks to critical infrastructure, considering both cyber and physical threats and the associated likelihoods, vulnerabilities, and consequences.

''(B) CONSULTATION.—In establishing the process required under subparagraph (A), the Secretary shall consult—

''(i) Sector Risk Management Agencies;

''(ii) critical infrastructure owners and operators;

''(iii) the Assistant to the President for National Security Affairs;

''(iv) the Assistant to the President for Homeland Security; and

''(v) the National Cyber Director.

''(C) PROCESS ELEMENTS.—The process established under subparagraph (A) shall include elements to—

''(i) collect relevant information, collected pursuant to section 2218, from Sector Risk Management Agencies relating to the threats, vulnerabilities, and consequences related to the particular sectors of those Sector Risk Management Agencies;

''(ii) allow critical infrastructure owners and operators to submit relevant information to the Secretary for consideration; and

''(iii) outline how the Secretary will solicit input from other Federal departments and agencies.

''(D) PUBLICATION.—Not later than 180 days after the date of enactment of this section, the Secretary shall publish in the Federal Register procedures for the process established under subparagraph (A), subject to any redactions the Secretary determines are necessary to protect classified or other sensitive information.

''(E) REPORT.—The Secretary shall submit to the President, 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 risks identified by the process established under subparagraph (A)—

''(i) not later than 1 year after the date of enactment of this section; and

''(ii) not later than 1 year after the date on which the Secretary submits a periodic evaluation described in section 9002(b)(2) of title XC of division H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 652a(b)(2)).

''(2) NATIONAL CRITICAL INFRASTRUCTURE RESILIENCE STRATEGY.—

''(A) IN GENERAL.—Not later than 1 year after the date on which the Secretary delivers each report required under paragraph (1), the President shall deliver to majority and minority leaders of the Senate, the Speaker and minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a national critical infrastructure resilience strategy designed to address the risks identified by the Secretary.

''(B) ELEMENTS.—Each strategy delivered under subparagraph (A) shall—

''(i) prioritize areas of risk to critical infrastructure that would compromise or disrupt national critical functions impacting national security, economic security, or public health and safety;

''(ii) assess the implementation of the previous national critical infrastructure resilience strategy, as applicable;

''(iii) identify and outline current and proposed national-level actions, programs, and efforts, including resource requirements, to be taken to address the risks identified;

''(iv) identify the Federal departments or agencies responsible for leading each national-level action, program, or effort and the relevant critical infrastructure sectors for each; and

''(v) request any additional authorities necessary to successfully execute the strategy.

''(C) FORM.—Each strategy delivered under subparagraph (A) shall be unclassified, but may contain a classified annex.

''(3) CONGRESSIONAL BRIEFING.—Not later than 1 year after the date on which the President delivers the first strategy required under paragraph (2)(A), and each year thereafter, the Secretary, in coordination with Sector Risk Management Agencies, shall brief the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives on—

''(A) the national risk management cycle activities undertaken pursuant to the strategy delivered under paragraph (2)(A); and

''(B) the amounts and timeline for funding that the Secretary has determined would be necessary to address risks and successfully execute the full range of activities proposed by the strategy delivered under paragraph (2)(A).''.

(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 item relating to section 2220E the following:

''Sec. 2220F. National risk management cycle.''.

Subtitle B—Securing Open Source Software Act of 2023

SEC. 6111. SHORT TITLE.

This subtitle may be cited as the ''Securing Open Source Software Act of 2023''.

SEC. 6112. FINDINGS.

Congress finds that—

(1) open source software fosters technology development and is an integral part of overall cybersecurity;

(2) a secure, healthy, vibrant, and resilient open source software ecosystem is crucial for ensuring the national security and economic vitality of the United States;

(3) open source software is part of the foundation of digital infrastructure that promotes a free and open internet;

(4) due to both the unique strengths of open source software and inconsistent historical investment in open source software security, there exist unique challenges in securing open source software; and

(5) the Federal Government should play a supporting role in ensuring the long-term security of open source software.

SEC. 6113. OPEN SOURCE SOFTWARE SECURITY DUTIES.

(a) IN GENERAL.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 650 et seq.), as amended by section 6102(a), is amended—

(1) in section 2200 (6 U.S.C. 650)—

(A) by redesignating paragraphs (22) through (28) as paragraphs (25) through (31), respectively; and

(B) by inserting after paragraph (21) the following:

''(22) OPEN SOURCE SOFTWARE.—The term 'open source software' means software for which the human-readable source code is made available to the public for use, study, re-use, modification, enhancement, and redistribution.

''(23) OPEN SOURCE SOFTWARE COMMUNITY.—The term 'open source software community' means the community of individuals, foundations, nonprofit organizations, corporations, and other entities that—

''(A) develop, contribute to, maintain, and publish open source software; or

''(B) otherwise work to ensure the security of the open source software ecosystem.

''(24) OPEN SOURCE SOFTWARE COMPONENT.—The term 'open source software component' means an individual repository of open source software that is made available to the public.'';

(2) in section 2202(c) (6 U.S.C. 652(c))—

(A) in paragraph (13), by striking ''and'' at the end;

(B) by redesignating paragraph (14) as paragraph (17); and

(C) by inserting after paragraph (13) the following:

''(14) support, including by offering services, the secure usage and deployment of software, including open source software, in the software development lifecycle at Federal agencies in accordance with section 2220G;''; and

(3) by adding at the end the following:

''SEC. 2220G. OPEN SOURCE SOFTWARE SECURITY DUTIES.

''(a) DEFINITION.—In this section, the term 'software bill of materials' has the meaning given the term in the Minimum Elements for a Software Bill of Materials published by the Department of Commerce, or any superseding definition published by the Agency.

''(b) EMPLOYMENT.—The Director shall, to the greatest extent practicable, employ individuals in the Agency who—

''(1) have expertise and experience participating in the open source software community; and

''(2) perform the duties described in subsection (c).

''(c) DUTIES OF THE DIRECTOR.—

''(1) IN GENERAL.—The Director shall—

''(A) perform outreach and engagement to bolster the security of open source software;

''(B) support Federal efforts to strengthen the security of open source software;

''(C) coordinate, as appropriate, with non-Federal entities on efforts to ensure the long-term security of open source software;

''(D) serve as a public point of contact regarding the security of open source software for non-Federal entities, including State, local, Tribal, and territorial partners, the private sector, international partners, and the open source software community; and

''(E) support Federal and non-Federal supply chain security efforts by encouraging efforts to bolster open source software security, such as—

''(i) assisting in coordinated vulnerability disclosures in open source software components pursuant to section 2209(n); and

''(ii) supporting the activities of the Federal Acquisition Security Council.

''(2) ASSESSMENT OF CRITICAL OPEN SOURCE SOFTWARE COMPONENTS.—

''(A) FRAMEWORK.—Not later than 1 year after the date of enactment of this section, the Director shall publicly publish a framework, incorporating government, industry, and open source software community frameworks and best practices, including those published by the National Institute of Standards and Technology, for assessing the risk of open source software components, including direct and indirect open source software dependencies, which shall incorporate, at a minimum—

''(i) the security properties of code in a given open source software component, such as whether the code is written in a memory-safe programming language;

''(ii) the security practices of development, build, and release processes of a given open source software component, such as the use of multi-factor authentication by maintainers and cryptographic signing of releases;

''(iii) the number and severity of publicly known, unpatched vulnerabilities in a given open source software component;

''(iv) the breadth of deployment of a given open source software component;

''(v) the level of risk associated with where a given open source software component is integrated or deployed, such as whether the component operates on a network boundary or in a privileged location; and

''(vi) the health of the open source software community for a given open source software component, including, where applicable, the level of current and historical investment and maintenance in the open source software component, such as the number and activity of individual maintainers.

''(B) UPDATING FRAMEWORK.—Not less frequently than annually after the date on which the framework is published under subparagraph (A), the Director shall—

''(i) determine whether updates are needed to the framework described in subparagraph (A), including the augmentation, addition, or removal of the elements described in clauses (i) through (vi) of such subparagraph; and

''(ii) if the Director determines that additional updates are needed under clause (i), make those updates to the framework.

''(C) DEVELOPING FRAMEWORK.—In developing the framework described in subparagraph (A), the Director shall consult with—

''(i) appropriate Federal agencies, including the National Institute of Standards and Technology;

''(ii) individuals and nonprofit organizations from the open source software community; and

''(iii) private companies from the open source software community.

''(D) USABILITY.—The Director shall ensure, to the greatest extent practicable, that the framework described in subparagraph (A) is usable by the open source software community, including through the consultation described in subparagraph (C).

''(E) FEDERAL OPEN SOURCE SOFTWARE ASSESSMENT.—Not later than 1 year after the publication of the framework described in subparagraph (A), and not less frequently than every 2 years thereafter, the Director shall, to the greatest extent practicable and using the framework described in subparagraph (A)—

''(i) perform an assessment of open source software components used directly or indirectly by Federal agencies based on readily available, and, to the greatest extent practicable, machine readable, information, such as—

''(I) software bills of materials that are, at the time of the assessment, made available to the Agency or are otherwise accessible via the internet;

''(II) software inventories, available to the Director at the time of the assessment, from the Continuous Diagnostics and Mitigation program of the Agency; and

''(III) other publicly available information regarding open source software components; and

''(ii) develop 1 or more ranked lists of components described in clause (i) based on the assessment, such as ranked by the criticality, level of risk, or usage of the components, or a combination thereof.

''(F) AUTOMATION.—The Director shall, to the greatest extent practicable, automate the assessment conducted under subparagraph (E).

''(G) PUBLICATION.—The Director shall publicly publish and maintain any tools developed to conduct the assessment described in subparagraph (E) as open source software.

''(H) SHARING.—

''(i) RESULTS.—The Director shall facilitate the sharing of the results of each assessment described in subparagraph (E)(i) with appropriate Federal and non-Federal entities working to support the security of open source software, including by offering means for appropriate Federal and non-Federal entities to download the assessment in an automated manner.

''(ii) DATASETS.—The Director may publicly publish, as appropriate, any datasets or versions of the datasets developed or consolidated as a result of an assessment described in subparagraph (E)(i).

''(I) CRITICAL INFRASTRUCTURE ASSESSMENT STUDY AND PILOT.—

''(i) STUDY.—Not later than 2 years after the publication of the framework described in subparagraph (A), the Director shall conduct a study regarding the feasibility of the Director conducting the assessment described in subparagraph (E) for critical infrastructure entities.

''(ii) PILOT.—

''(I) IN GENERAL.—If the Director determines that the assessment described in clause (i) is feasible, the Director may conduct a pilot assessment on a voluntary basis with 1 or more critical infrastructure sectors, in coordination with the Sector Risk Management Agency and the sector coordinating council of each participating sector.

''(II) TERMINATION.—If the Director proceeds with the pilot described in subclause (I), the pilot shall terminate on the date that is 2 years after the date on which the Director begins the pilot.

''(iii) REPORTS.—

''(I) STUDY.—Not later than 180 days after the date on which the Director completes the study conducted under clause (i), the Director shall submit to the appropriate congressional committees a report that—

''(aa) summarizes the study; and

''(bb) states whether the Director plans to proceed with the pilot described in clause (ii)(I).

''(II) PILOT.—If the Director proceeds with the pilot described in clause (ii), not later than 1 year after the date on which the Director begins the pilot, the Director shall submit to the appropriate congressional committees a report that includes—

''(aa) a summary of the results of the pilot; and

''(bb) a recommendation as to whether the activities carried out under the pilot should be continued after the termination of the pilot described in clause (ii)(II).

''(3) COORDINATION WITH NATIONAL CYBER DIRECTOR.—The Director shall—

''(A) brief the National Cyber Director on the activities described in this subsection; and

''(B) coordinate activities with the National Cyber Director, as appropriate.

''(4) REPORTS.—

''(A) IN GENERAL.—Not later than 1 year after the date of enactment of this section, and every 2 years thereafter, the Director shall submit to the appropriate congressional committees a report that includes—

''(i) a summary of the work on open source software security performed by the Director during the period covered by the report, including a list of the Federal and non-Federal entities with which the Director interfaced;

''(ii) the framework developed under paragraph (2)(A);

''(iii) a summary of any updates made to the framework developed under paragraph (2)(A) pursuant to paragraph (2)(B) since the last report submitted under this subparagraph;

''(iv) a summary of each assessment conducted pursuant to paragraph (2)(E) since the last report was submitted under this subparagraph;

''(v) a summary of changes made to the assessment conducted pursuant to paragraph (2)(E) since the last report submitted under this subparagraph, including overall security trends; and

''(vi) a summary of the types of entities with which an assessment conducted pursuant to paragraph (2)(E) since the last reported submitted under this subparagraph was shared pursuant to paragraph (2)(H), including a list of the Federal and non-Federal entities with which the assessment was shared.

''(B) PUBLIC REPORT.—Not later than 30 days after the date on which the Director submits a report required under subparagraph (A), the Director shall make a version of the report publicly available on the website of the Agency.''.

(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), as amended by section 6102(b), is amended by inserting after the item relating to section 2220F the following:

''Sec. 2220G. Open source software security duties.''.

SEC. 6114. SOFTWARE SECURITY ADVISORY SUBCOMMITTEE.

Section 2219(d)(1) of the Homeland Security Act of 2002 (6 U.S.C. 665e(d)(1)) is amended by adding at the end the following:

''(E) Software security, including open source software security.''.

SEC. 6115. OPEN SOURCE SOFTWARE GUIDANCE.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEE.—The term ''appropriate congressional committee'' has the meaning given the term in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101).

(2) COVERED AGENCY.—The term ''covered agency'' means an agency described in section 901(b) of title 31, United States Code.

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

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

(5) OPEN SOURCE SOFTWARE; OPEN SOURCE SOFTWARE COMMUNITY.—The terms ''open source software'' and ''open source software community'' have the meanings given those terms in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650), as amended by section 6113.

(b) GUIDANCE.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Director, in coordination with the National Cyber

Director, the Director of the Cybersecurity and Infrastructure Security Agency, and the Administrator of General Services, shall issue guidance on the responsibilities of the chief information officer at each covered agency regarding open source software, which shall include—

(A) how chief information officers at each covered agency should, considering industry and open source software community best practices—

(i) manage and reduce risks of using open source software; and

(ii) guide contributing to and releasing open source software;

(B) how chief information officers should enable, rather than inhibit, the secure usage of open source software at each covered agency;

(C) any relevant updates to the Memorandum M–16–21 issued by the Office of Management and Budget on August 8, 2016, entitled, ''Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software''; and

(D) how covered agencies may contribute publicly to open source software that the covered agency uses, including how chief information officers should encourage those contributions.

(2) EXEMPTION OF NATIONAL SECURITY SYSTEMS.—The guidance issued under paragraph (1) shall not apply to national security systems.

(c) PILOT.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the chief information officer of each covered agency selected under paragraph (2), in coordination with the Director, the National Cyber Director, the Director of the Cybersecurity and Infrastructure Security Agency, and the Administrator of General Services, shall establish a pilot open source function at the covered agency that—

(A) is modeled after open source program offices, such as those in the private sector, the nonprofit sector, academia, and other non-Federal entities; and

(B) shall—

(i) support the secure usage of open source software at the covered agency;

(ii) develop policies and processes for contributions to and releases of open source software at the covered agency, in consultation, as appropriate, with the offices of general counsel and procurement of the covered agency;

(iii) interface with the open source software community; and

(iv) manage and reduce risks of using open source software at the covered agency.

(2) SELECTION OF PILOT AGENCIES.—The Director, in coordination with the National Cyber Director, the Director of the Cybersecurity and Infrastructure Security Agency, and the Administrator of General Services, shall select not less than 1 and not more than 5 covered agencies to conduct the pilot described in paragraph (1).

(3) ASSESSMENT.—Not later than 1 year after the establishment of the pilot open source functions described in paragraph (1), the Director, in coordination with the National Cyber Director, the Director of the Cybersecurity and Infrastructure Security Agency, and the Administrator of General Services, shall assess whether open source functions should be established at some or all covered agencies, including—

(A) how to organize those functions within covered agencies, such as the creation of open source program offices; and

(B) appropriate roles and responsibilities for those functions.

(4) GUIDANCE.—Notwithstanding the termination of the pilot open source functions under paragraph (5), if the Director determines, based on the assessment described in paragraph (3), that some or all of the open source functions should be established at some or all covered agencies, the Director, in coordination with the National Cyber Director, the Director of the Cybersecurity and Infrastructure Security Agency, and the Administrator of General Services, shall issue guidance on the implementation of those functions.

(5) TERMINATION.—The pilot open source functions described in paragraph (1) shall terminate not later than 4 years after the establishment of the pilot open source functions.

(d) BRIEFING AND REPORT.—The Director shall—

(1) not later than 1 year after the date of enactment of this Act, brief the appropriate congressional committees on the guidance issued under subsection (b); and

(2) not later than 540 days after the establishment of the pilot open source functions under subsection (c)(1), submit to the appropriate congressional committees a report on—

(A) the pilot open source functions; and

(B) the results of the assessment conducted under subsection (c)(3).

(e) DUTIES.—Section 3554(b) of title 44, United States Code, as amended by section 5103, is amended by inserting after paragraph (7) the following:

''(8) plans and procedures to ensure the secure usage and development of software, including open source software (as defined in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650));''.

SEC. 6116. RULE OF CONSTRUCTION.

Nothing in this subtitle or the amendments made by this subtitle shall be construed to provide any additional regulatory authority to any Federal agency described therein.

Subtitle C—Offices of Countering Weapons of Mass Destruction and Health Security Act of 2023

SEC. 6121. SHORT TITLE.

This subtitle may be cited as the ''Offices of Countering Weapons of Mass Destruction and Health Security Act of 2023''.

CHAPTER 1—COUNTERING WEAPONS OF MASS DESTRUCTION OFFICE

SEC. 6122. COUNTERING WEAPONS OF MASS DESTRUCTION OFFICE.

(a) HOMELAND SECURITY ACT OF 2002.—Title XIX of the Homeland Security Act of 2002 (6 U.S.C. 590 et seq.) is amended—

(1) in section 1901 (6 U.S.C. 591)—

(A) in subsection (c), by striking paragraphs (1) and (2) and inserting the following:

''(1) matters and strategies pertaining to—

''(A) weapons of mass destruction; and

''(B) non-medical aspects of chemical, biological, radiological, nuclear, and other related emerging threats;

''(2) coordinating the efforts of the Department to counter—

''(A) weapons of mass destruction; and

''(B) non-medical aspects of chemical, biological, radiological, nuclear, and other related emerging threats; and

''(3) enhancing the ability of Federal, State, local, and Tribal partners to prevent, detect, protect against, and mitigate the impacts of terrorist attacks in the United States to counter—

''(A) weapons of mass destruction; and

''(B) non-medical aspects of use of unauthorized chemical, biological, radiological, and nuclear materials, devices, or agents and other related emerging threats.''; and

(B) by striking subsection (e);

(2) by amending section 1921 (6 U.S.C. 591g) to read as follows:

''SEC. 1921. MISSION OF THE OFFICE.

''The Office shall be responsible for—

''(1) coordinating the efforts of the Department and with other Federal departments and agencies to counter—

''(A) weapons of mass destruction; and

''(B) chemical, biological, radiological, nuclear, and other related emerging threats; and

''(2) enhancing the ability of Federal, State, local, and Tribal partners to prevent, detect, protect against, and mitigate the impacts of attacks using—

''(A) weapons of mass destruction against the United States; or

''(B) unauthorized chemical, biological, radiological, nuclear materials, devices, or agents or other related emerging threats against the United States.'';

(3) in section 1922 (6 U.S.C. 591h)—

(A) by striking subsection (b); and

(B) by redesignating subsection (c) as subsection (b);

(4) in section 1923 (6 U.S.C. 592)—

(A) by redesignating subsections (a) and (b) as subsections (b) and (d), respectively;

(B) by inserting before subsection (b), as so redesignated, the following:

''(a) OFFICE RESPONSIBILITIES.—

''(1) IN GENERAL.—For the purposes of coordinating the efforts of the Department to counter weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats, the Office shall—

''(A) provide expertise and guidance to Department leadership and components on nonmedical aspects of chemical, biological, radiological, nuclear, and other related emerging threats, subject to the research, development, testing, and evaluation coordination requirement described in subparagraph (G);

''(B) in coordination with the Office for Strategy, Policy, and Plans, lead development of policies and strategies to counter weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats on behalf of the Department;

''(C) identify, assess, and prioritize capability gaps relating to the strategic and mission objectives of the Department for weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats;

''(D) in coordination with the Office of Intelligence and Analysis, support components of the Department, and Federal, State, local, and Tribal partners by providing intelligence and information analysis and reports on weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats;

''(E) in consultation with the Science and Technology Directorate, assess risk to the United States from weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats;

''(F) lead development and prioritization of Department requirements to counter weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats, subject to the research, development, testing, and evaluation coordination requirement described in subparagraph (G), which requirements shall be—

''(i) developed in coordination with end users; and

''(ii) reviewed by the Joint Requirements Council, as directed by the Secretary;

''(G) in coordination with the Science and Technology Directorate, direct, fund, and coordinate capability development activities to counter weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats research, development, test, and evaluation matters, including research, development, testing,

and evaluation expertise, threat characterization, technology maturation, prototyping, and technology transition;

''(H) acquire, procure, and deploy capabilities to counter weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats, and serve as the lead advisor of the Department on component acquisition, procurement, and deployment of counter-weapons of mass destruction capabilities;

''(I) in coordination with the Office of Health Security, support components of the Department, and Federal, State, local, and Tribal partners on chemical, biological, radiological, nuclear, and other related emerging threats health matters;

''(J) provide expertise on weapons of mass destruction and non-medical aspects of chemical, biological, radiological, nuclear, and other related emerging threats to Departmental and Federal partners to support engagements and efforts with international partners subject to the research, development, testing, and evaluation coordination requirement under subparagraph (G); and

''(K) carry out any other duties assigned to the Office by the Secretary.

''(2) DETECTION AND REPORTING.—For purposes of the detection and reporting responsibilities of the Office for weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats, the Office shall—

''(A) in coordination with end users, including State, local, and Tribal partners, as appropriate—

''(i) carry out a program to test and evaluate technology, in consultation with the Science and Technology Directorate, to detect and report on weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats, in coordination with other Federal agencies, as appropriate, and establish performance metrics to evaluate the effectiveness of individual detectors and detection systems in detecting those weapons of mass destruction or chemical, biological, radiological, nuclear, or other related emerging threats—

''(I) under realistic operational and environmental conditions; and

''(II) against realistic adversary tactics and countermeasures;

''(B) in coordination with end users, conduct, support, coordinate, and encourage a transformational program of research and development to generate and improve technologies to detect, protect against, and report on the illicit entry, transport, assembly, or potential use within the United States of weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats, and coordinate with the Under Secretary for Science and Technology on research and development efforts relevant to the mission of the Office and the Under Secretary for Science and Technology;

''(C) before carrying out operational testing under subparagraph (A), develop a testing and evaluation plan that articulates the requirements for the user and describes how these capability needs will be tested in developmental test and evaluation and operational test and evaluation;

''(D) as appropriate, develop, acquire, and deploy equipment to detect and report on weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats in support of Federal, State, local, and Tribal governments;

''(E) support and enhance the effective sharing and use of appropriate information on weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats generated by elements of the intelligence community, law enforcement agencies, other Federal agencies, State, local, and Tribal governments, and foreign governments, as well as provide appropriate information to those entities;

''(F) consult, as appropriate, with relevant Departmental components and offices, the Department of Health and Human Services, and other Federal partners, on weapons of mass destruction and non-medical aspects of chemical, biological, radiological, nuclear, and other related emerging threats and efforts to mitigate, prepare, and respond to all threats in support of the State, local, and Tribal communities; and

''(G) perform other duties as assigned by the Secretary.'';

(C) in subsection (b), as so redesignated—

(i) in the subsection heading, by striking ''MISSION'' and inserting ''RADIOLOGICAL AND NUCLEAR RESPONSIBILITIES'';

(ii) in paragraph (1)—

(I) by inserting ''deploy,'' after ''acquire,''; and

(II) by striking ''deployment'' and inserting ''operation'';

(iii) by striking paragraphs (6) through (10);

(iv) redesignating paragraphs (11) and (12) as paragraphs (6) and (7), respectively;

(v) in paragraph (6), as so redesignated—

(I) by striking subparagraph (B);

(II) by striking ''activities—'' and all that follows through ''to ensure'' and inserting ''activities to ensure''; and

(III) by striking ''attacks; and'' and inserting ''attacks;'';

(vi) in paragraph (7)(C)(v), as so redesignated—

(I) in the matter preceding subclause (I), by inserting ''except as otherwise provided,'' before ''require''; and

(II) in subclause (II)—

(aa) in the matter preceding item (aa), by striking ''death or disability'' and inserting ''death, disability, or a finding of good cause as determined by the Assistant Secretary (including extreme hardship, extreme need, or the needs of the Office) and for which the Assistant Secretary may grant a waiver of the repayment obligation''; and

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

(vii) by striking paragraph (13); and

(viii) by redesignating paragraph (14) as paragraph (8); and

(D) by inserting after subsection (b), as so redesignated, the following:

''(c) CHEMICAL AND BIOLOGICAL RESPONSIBILITIES.—The Office—

''(1) shall be responsible for coordinating with other Federal efforts to enhance the ability of Federal, State, local, and Tribal governments to prevent, detect, mitigate, and protect against the importation, possession, storage, transportation, development, or use of unauthorized chemical and biological materials, devices, or agents against the United States; and

''(2) shall—

''(A) serve as a primary entity responsible for the efforts of the Department to develop, acquire, deploy, and support the operations of a national biological detection system and improve that system over time;

''(B) enhance the chemical and biological detection efforts of Federal, State, local, and Tribal governments and provide guidance, tools, and training to help ensure a managed, coordinated response; and

''(C) collaborate with the Department of Health and Human Services, the Office of Health Security of the Department, the Defense Advanced Research Projects Agency, the National Aeronautics and Space Administration, and other relevant Federal stakeholders, and receive input from industry, academia, and the national laboratories on chemical and biological surveillance efforts.'';

(5) in section 1924 (6 U.S.C. 593), by striking ''section 11011 of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 (5 U.S.C. 3104 note).'' and inserting ''section 4092 of title 10, United States Code, except that the authority shall be limited to facilitate the recruitment of experts in the chemical, biological, radiological, or nuclear specialties.'';

(6) in section 1927(a)(1)(C) (6 U.S.C. 596a(a)(1)(C))—

(A) in clause (i), by striking ''required under section 1036 of the National Defense Authorization Act for Fiscal Year 2010'';

(B) in clause (ii), by striking ''and'' at the end;

(C) in clause (iii), by striking the period at the end and inserting ''; and''; and

(D) by adding at the end the following:

''(iv) includes any other information regarding national technical nuclear forensics activities carried out under section 1923.'';

(7) in section 1928 (6 U.S.C. 596b)—

(A) in subsection (a), by striking ''high-risk urban areas'' and inserting ''jurisdictions designated under subsection (c)'';

(B) in subsection (c)(1), by striking ''from among high-risk urban areas under section 2003'' and inserting ''based on the capability and capacity of the jurisdiction, as well as the relative threat, vulnerability, and consequences from terrorist attacks and other high-consequence events utilizing nuclear or other radiological materials''; and

(C) by striking subsection (d) and inserting the following:

''(d) REPORT.—Not later than 2 years after the date of enactment of the Offices of Countering Weapons of Mass Destruction and Health Security Act of 2023, the Secretary shall submit to the appropriate congressional committees an update on the STC program.''; and

(8) by inserting after section 1928 (6 U.S.C. 596b) the following:

''SEC. 1929. ACCOUNTABILITY.

''(a) DEPARTMENTWIDE STRATEGY.—

''(1) IN GENERAL.—Not later than 180 days after the date of enactment of Offices of Countering Weapons of Mass Destruction and Health Security Act of 2023, and every 4 years thereafter, the Secretary shall create a Departmentwide strategy and implementation plan to counter weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats, which should—

''(A) have clearly identified authorities, specified roles, objectives, benchmarks, accountability, and timelines;

''(B) incorporate the perspectives of non-Federal and private sector partners; and

''(C) articulate how the Department will contribute to relevant national-level strategies and work with other Federal agencies.

''(2) CONSIDERATION.—The Secretary shall appropriately consider weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats when creating the strategy and implementation plan required under paragraph (1).

''(3) REPORT.—The Office shall submit to the appropriate congressional committees a report on the updated Departmentwide strategy and implementation plan required under paragraph (1).

''(b) DEPARTMENTWIDE BIODEFENSE REVIEW AND STRATEGY.—

''(1) IN GENERAL.—Not later than 180 days after the date of enactment of the Offices of Countering Weapons of Mass Destruction and Health Security Act of 2023, the Secretary, in consultation with appropriate stakeholders representing Federal, State, local,

Tribal, academic, private sector, and nongovernmental entities, shall conduct a Departmentwide review of biodefense activities and strategies.

''(2) REVIEW.—The review required under paragraph (1) shall—

''(A) identify with specificity the biodefense lines of effort of the Department, including biodefense lines of effort relating to biodefense roles, responsibilities, and capabilities of components and offices of the Department;

''(B) assess how such components and offices coordinate internally and with public and private partners in the biodefense enterprise;

''(C) identify any policy, resource, capability, or other gaps in the Department's ability to assess, prevent, protect against, and respond to biological threats;

''(D) identify any organizational changes or reforms necessary for the Department to effectively execute its biodefense mission and role, including with respect to public and private partners in the biodefense enterprise; and

''(E) assess the risk of high-risk gain-of-function research to the homeland security of the United States and identify the gaps in the response of the Department to that risk.

''(3) STRATEGY.—Not later than 1 year after completion of the review required under paragraph (1), the Secretary shall issue a biodefense strategy for the Department that—

''(A) is informed by such review and is aligned with section 1086 of the National Defense Authorization Act for Fiscal Year 2017 (6 U.S.C. 104; relating to the development of a national biodefense strategy and associated implementation plan, including a review and assessment of biodefense policies, practices, programs, and initiatives) or any successor strategy; and

''(B) shall—

''(i) describe the biodefense mission and role of the Department, as well as how such mission and role relates to the biodefense lines of effort of the Department;

''(ii) clarify, as necessary, biodefense roles, responsibilities, and capabilities of the components and offices of the Department involved in the biodefense lines of effort of the Department;

''(iii) establish how biodefense lines of effort of the Department are to be coordinated within the Department;

''(iv) establish how the Department engages with public and private partners in the biodefense enterprise, including other Federal agencies, national laboratories and sites, and State, local, and Tribal entities, with specificity regarding the frequency and nature of such engagement by Department components and offices with State, local, and Tribal entities; and

''(v) include information relating to—

''(I) milestones and performance metrics that are specific to the biodefense mission and role of the Department described in clause (i); and

''(II) implementation of any operational changes necessary to carry out clauses (iii) and (iv).

''(4) PERIODIC UPDATE.—Beginning not later than 5 years after the issuance of the biodefense strategy and implementation plans required under paragraph (3), and not less often than once every 5 years thereafter, the Secretary shall review and update, as necessary, such strategy and plans.

''(5) CONGRESSIONAL OVERSIGHT.—Not later than 30 days after the issuance of the biodefense strategy and implementation plans required under paragraph (3), the Secretary shall brief the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives regarding such strategy and plans.

''(c) EMPLOYEE MORALE.—Not later than 180 days after the date of enactment of the Offices of Countering Weapons of Mass Destruction and Health Security Act of 2023, the Office shall submit to and brief the appropriate congressional committees on a strategy and plan to continuously improve morale within the Office.

''(d) COMPTROLLER GENERAL.—Not later than 1 year after the date of enactment of the Offices of Countering Weapons of Mass Destruction and Health Security Act of 2023, the Comptroller General of the United States shall conduct a review of and brief the appropriate congressional committees on—

''(1) the efforts of the Office to prioritize the programs and activities that carry out the mission of the Office, including research and development;

''(2) the consistency and effectiveness of stakeholder coordination across the mission of the Office, including operational and support components of the Department and State and local entities; and

''(3) the efforts of the Office to manage and coordinate the lifecycle of research and development within the Office and with other components of the Department, including the Science and Technology Directorate.

''(e) NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE.—

''(1) STUDY.—The Secretary shall enter into an agreement with the National Academies of Sciences, Engineering, and Medicine to conduct a consensus study and report to the Secretary and the appropriate congressional committees on—

''(A) the role of the Department in preparing, detecting, and responding to biological and health security threats to the homeland;

''(B) recommendations to improve departmental biosurveillance efforts against biological threats, including any relevant biological detection methods and technologies; and

''(C) the feasibility of different technological advances for biodetection compared to the cost, risk reduction, and timeliness of those advances.

''(2) BRIEFING.—Not later than 1 year after the date on which the Secretary receives the report required under paragraph (1), the Secretary shall brief the appropriate congressional committees on—

''(A) the implementation of the recommendations included in the report; and

''(B) the status of biological detection at the Department, and, if applicable, timelines for the transition to updated technology.

''(f) ADVISORY COUNCIL.—

''(1) ESTABLISHMENT.—Not later than 180 days after the date of enactment of the Offices of Countering Weapons of Mass Destruction and Health Security Act of 2023, the Secretary shall establish an advisory body to advise on the ongoing coordination of the efforts of the Department to counter weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats, to be known as the Advisory Council for Countering Weapons of Mass Destruction (in this subsection referred to as the 'Advisory Council').

''(2) MEMBERSHIP.—The members of the Advisory Council shall—

''(A) be appointed by the Assistant Secretary; and

''(B) to the extent practicable, represent a geographic (including urban and rural) and substantive cross section of officials from State, local, and Tribal governments, academia, the private sector, national laboratories, and nongovernmental organizations, including, as appropriate—

''(i) members selected from the emergency management field and emergency response providers;

''(ii) State, local, and Tribal government officials;

''(iii) experts in the public and private sectors with expertise in chemical, biological, radiological, or nuclear materials, devices, or agents;

''(iv) representatives from the national laboratories; and

''(v) such other individuals as the Assistant Secretary determines to be appropriate.

''(3) RESPONSIBILITIES.— The Advisory Council shall—

''(A) advise the Assistant Secretary on all aspects of countering weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats;

''(B) incorporate State, local, and Tribal government, national laboratories, and private sector input in the development of the strategy and implementation plan of the Department for countering weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats; and

''(C) provide advice on performance criteria for a national biological detection system and review the testing protocol for biological detection prototypes.

''(4) CONSULTATION.—To ensure input from and coordination with State, local, and Tribal governments, the Assistant Secretary shall regularly consult and work with the Advisory Council on the administration of Federal assistance provided by the Department, including with respect to the development of requirements of Office programs, as appropriate.

''(5) VOLUNTARY SERVICE.—The members of the Advisory Council shall serve on the Advisory Council on a voluntary basis.

''(6) FACA.—Chapter 10 of title 5, United States Code, shall not apply to the Advisory Council.

''(7) QUALIFICATIONS.—Each member of the Advisory Council shall—

''(A) be impartial in any advice provided to the Advisory Council; and

''(B) not seek to advance any political position or predetermined conclusion as a member of the Advisory Council.''.

(b) COUNTERING WEAPONS OF MASS DESTRUCTION ACT OF 2018.—Section 2 of the Countering Weapons of Mass Destruction Act of 2018 (Public Law 115–387; 132 Stat. 5162) is amended—

(1) in subsection (b)(2) (6 U.S.C. 591 note), by striking ''1927'' and inserting ''1926''; and

(2) in subsection (g) (6 U.S.C. 591 note)—

(A) in the matter preceding paragraph (1), by striking ''one year after the date of the enactment of this Act, and annually thereafter,'' and inserting ''June 30 of each year,''; and

(B) in paragraph (2), by striking ''Security, including research and development activities'' and inserting ''Security''.

(c) SECURITY AND ACCOUNTABILITY FOR EVERY PORT ACT OF 2006.—The Security and Accountability for Every Port Act of 2006 (Public Law 109–347; 120 Stat 1884) is amended—

(1) in section 1(b), by striking the item relating to section 502; and

(2) by striking section 502 (6 U.S.C. 592a).

SEC. 6123. RULE OF CONSTRUCTION.

Nothing in this chapter or the amendments made by this chapter may be construed as modifying any existing authority under any provision of law not expressly amended by this chapter.

CHAPTER 2—OFFICE OF HEALTH SECURITY

SEC. 6124. OFFICE OF HEALTH SECURITY.

(a) ESTABLISHMENT.—The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

(1) in section 103 (6 U.S.C. 113)—

(A) in subsection (a)(2)—

(i) by striking ''the Assistant Secretary for Health Affairs,''; and

(ii) by striking ''Affairs, or'' and inserting ''Affairs or''; and

(B) in subsection (d), by adding at the end the following:

''(6) A Chief Medical Officer.'';

(2) by adding at the end the following:

''TITLE XXIII—OFFICE OF HEALTH SECURITY'';

(3) by redesignating section 1931 (6 U.S.C. 597) as section 2301 and transferring such section to appear after the heading for title XXIII, as added by paragraph (2);

(4) in section 2301, as so redesignated—

(A) in the section heading, by striking ''**CHIEF MEDICAL OFFICER**'' and inserting ''**OFFICE OF HEALTH SECURITY**'';

(B) by striking subsections (a) and (b) and inserting the following:

''(a) IN GENERAL.—There is established in the Department an Office of Health Security.

''(b) HEAD OF OFFICE OF HEALTH SECURITY.—The Office of Health Security shall be headed by a chief medical officer, who shall—

''(1) be the Assistant Secretary for Health Security and the Chief Medical Officer of the Department;

''(2) be a licensed physician possessing a demonstrated ability in and knowledge of medicine and public health;

''(3) be appointed by the President; and

''(4) report directly to the Secretary.'';

(C) in subsection (c)—

(i) in the matter preceding paragraph (1), by striking ''medical issues related to natural disasters, acts of terrorism, and other man-made disasters'' and inserting ''medical activities of the Department and all workforce-focused health and safety activities of the Department'';

(ii) in paragraph (1), by striking '', the Administrator of the Federal Emergency Management Agency, the Assistant Secretary, and other Department officials'' and inserting ''and all other Department officials'';

(iii) in paragraph (4), by striking ''and'' at the end;

(iv) by redesignating paragraph (5) as paragraph (13); and

(v) by inserting after paragraph (4) the following:

''(5) overseeing all medical activities of the Department, including the delivery, advisement, and support of direct patient care and the organization, management, and staffing of component operations that deliver direct patient care;

''(6) advising the head of each component of the Department that delivers direct patient care regarding the recruitment and appointment of a component chief medical officer and deputy chief medical officer or the employees who function in the capacity of chief medical officer and deputy chief medical officer;

''(7) advising the Secretary and the head of each component of the Department that delivers direct patient care regarding knowledge and skill standards for medical personnel and the assessment of that knowledge and skill;

''(8) in coordination with the Chief Privacy Officer of the Department and the Chief Information Officer of the Department, advising the Secretary and the head of each component of the Department that delivers patient care regarding the collection, storage, and oversight of medical records;

''(9) with respect to any psychological health counseling or assistance program of the Department, including such a program of a law enforcement, operational, or support component of the Department, advising the head of each such component with such a program regarding—

''(A) ensuring such program includes safeguards against adverse actions by such component with respect to any employee solely because the employee identifies a need for psychological health counseling or assistance or receives such assistance;

''(B) ensuring such program includes safeguards regarding automatic referrals for employment-related examinations or inquires that are based solely on an employee who self identifies a need for psychological health counseling or assistance or receives such counseling or assistance, except that such safeguards shall not prevent a component referral to evaluate the ability of an employee to meet established medical or psychological standards by such component or to evaluate the national security eligibility of the employee;

''(C) increasing the availability and number of local psychological health professionals with experience providing psychological support services to personnel;

''(D) establishing a behavioral health curriculum for employees at the beginning of their careers to provide resources early regarding the importance of psychological health;

''(E) establishing periodic management training on crisis intervention and such component's psychological health counseling or assistance program;

''(F) improving any associated existing employee peer support programs, including by making additional training and resources available for peer support personnel in the workplace across such component;

''(G) developing and implementing a voluntary alcohol treatment program that includes a safe harbor for employees who seek treatment;

''(H) prioritizing, as appropriate, expertise in the provision of psychological health counseling and assistance for certain populations of the workforce, such as employees serving in positions within law enforcement, to help improve outcomes for those employees receiving that counseling or assistance; and

''(I) including, when appropriate, collaborating and partnering with key employee stakeholders and, for those components with employees with an exclusive representative, the exclusive representative with respect to such a program;

''(10) in consultation with the Chief Information Officer of the Department—

''(A) identifying methods and technologies for managing, updating, and overseeing patient records; and

''(B) setting standards for technology used by the components of the Department regarding the collection, storage, and oversight of medical records;

''(11) advising the Secretary and the head of each component of the Department that delivers direct patient care regarding contracts for the delivery of direct patient care, other medical services, and medical supplies;

''(12) coordinating with—

''(A) the Countering Weapons of Mass Destruction Office;

''(B) other components of the Department as directed by the Secretary;

''(C) Federal agencies, including the Department of Agriculture, the Department of Health and Human Services, the Department of State, and the Department of Transportation;

''(D) State, local, and Tribal governments; and

''(E) the medical community; and''; and

(D) by adding at the end the following:

''(d) ASSISTANCE AND AGREEMENTS.—The Secretary, acting through the Chief Medical Officer, in support of the medical activities of the Department, may—

''(1) provide technical assistance, training, and information to State, local, and Tribal governments and nongovernmental organizations;

''(2) enter into agreements with other Federal agencies; and

''(3) accept services from personnel of components of the Department and other Federal agencies on a reimbursable or nonreimbursable basis.

''(e) OFFICE OF HEALTH SECURITY PRIVACY OFFICER.—There shall be a Privacy Officer in the Office of Health Security with primary responsibility for privacy policy and compliance within the Office, who shall—

''(1) report directly to the Chief Medical Officer; and

''(2) ensure privacy protections are integrated into all Office of Health Security activities, subject to the review and approval of the Chief Privacy Officer of the Department to the extent consistent with the authority of the Chief Privacy Officer of the Department under section 222.

''(f) ACCOUNTABILITY.—

''(1) STRATEGY AND IMPLEMENTATION PLAN.—Not later than 180 days after the date of enactment of this subsection, and every 4 years thereafter, the Secretary shall create a Departmentwide strategy and implementation plan to address medical activities of, and the workforce health and safety matters under the purview of, the Department.

''(2) BRIEFING.—Not later than 90 days after the date of enactment of this subsection, the Secretary shall brief the appropriate congressional committees on the organizational transformations of the Office of Health Security, including how best practices were used in the creation of the Office of Health Security.'';

(5) by redesignating section 710 (6 U.S.C. 350) as section 2302 and transferring such section to appear after section 2301, as so redesignated;

(6) in section 2302, as so redesignated—

(A) in the section heading, by striking ''**MEDICAL SUPPORT**'' and inserting ''**SAFETY**'';

(B) in subsection (a), by striking ''Under Secretary for Management'' each place that term appears and inserting ''Chief Medical Officer''; and

(C) in subsection (b)—

(i) in the matter preceding paragraph (1), by striking ''Under Secretary for Management, in coordination with the Chief Medical Officer,'' and inserting ''Chief Medical Officer''; and

(ii) in paragraph (3), by striking ''as deemed appropriate by the Under Secretary,'';

(7) by redesignating section 528 (6 U.S.C. 321q) as section 2303 and transferring such section to appear after section 2302, as so redesignated;

(8) in section 2303, as so redesignated—

(A) in subsection (a), by striking ''Assistant Secretary for the Countering Weapons of Mass Destruction Office'' and inserting ''Chief Medical Officer''; and

(B) in subsection (b)—

(i) in paragraph (1), by striking ''Homeland Security Presidential Directive 9–Defense of the United States Agriculture and Food'' and inserting ''National Security Memorandum 16—Strengthening the Security and Resilience of the United States Food and Agriculture''; and

(ii) in paragraph (6), by inserting ''the Department of Agriculture and other'' before ''appropriate'';

(9) by redesignating section 1932 (6 U.S.C. 597a) as section 2304 and transferring such section to appear after section 2303, as so redesignated;

(10) in section 2304(f)(2)(B), as so redesignated, by striking ''Office of the Assistant Secretary for Preparedness and Response'' and inserting ''Administration for Strategic Preparedness and Response''; and

(11) by inserting after section 2304, as so redesignated, the following:

''SEC. 2305. RULES OF CONSTRUCTION.

''Nothing in this title shall be construed to—

''(1) override or otherwise affect the requirements described in section 888;

''(2) require the advice of the Chief Medical Officer on the appointment of Coast Guard officers or the officer from the Public Health Service of the Department of Health and Human Services assigned to the Coast Guard;

''(3) provide the Chief Medical Officer with authority to take any action that would diminish the interoperability of the Coast Guard medical system with the medical systems of the other branches of the Armed Forces of the United States; or

''(4) affect or diminish the authority of the Secretary of Health and Human Services or to grant to the Chief Medical Officer any authority that is vested in, or delegated to, the Secretary of Health and Human Services.''.

(b) TRANSITION AND TRANSFERS.—

(1) TRANSITION.—The individual appointed pursuant to section 1931 of the Homeland Security Act of 2002 (6 U.S.C. 597) of the Department of Homeland Security, as in effect on the day before the date of enactment of this Act, and serving as the Chief Medical Officer of the Department of Homeland Security on the day before the date of enactment of this Act, shall continue to serve as the Chief Medical Officer of the Department on and after the date of enactment of this Act without the need for reappointment.

(2) TRANSFER.—The Secretary of Homeland Security shall transfer to the Chief Medical Officer of the Department of Homeland Security—

(A) all functions, personnel, budget authority, and assets of the Under Secretary for Management relating to workforce health and safety, as in existence on the day before the date of enactment of this Act;

(B) all functions, personnel, budget authority, and assets of the Assistant Secretary for the Countering Weapons of Mass Destruction Office relating to the Chief Medical Officer, including the Medical Operations Directorate of the Countering Weapons of Mass Destruction Office, as in existence on the day before the date of enactment of this Act; and

(C) all functions, personnel, budget authority, and assets of the Assistant Secretary for the Countering Weapons of Mass Destruction Office associated with the efforts pertaining to the program coordination activities relating to defending the food, agriculture, and veterinary defenses of the Office, as in existence on the day before the date of enactment of this Act.

SEC. 6125. CONFIDENTIALITY OF MEDICAL QUALITY ASSURANCE RECORDS.

Title XXIII of the Homeland Security Act of 2002, as added by this chapter, is amended by adding at the end the following:

''SEC. 2306. CONFIDENTIALITY OF MEDICAL QUALITY ASSURANCE RECORDS.

''(a) DEFINITIONS.—In this section:

''(1) HEALTH CARE PROVIDER.—The term 'health care provider' means an individual who—

''(A) is—

''(i) an employee of the Department;

''(ii) a detailee to the Department from another Federal agency;

''(iii) a personal services contractor of the Department; or

''(iv) hired under a contract for services with the Department;

''(B) performs health care services as part of duties of the individual in that capacity; and

''(C) has a current, valid, and unrestricted license or certification—

''(i) that is issued by a State; and

''(ii) that is for the practice of medicine, osteopathic medicine, dentistry, nursing, emergency medical services, or another health profession.

''(2) MEDICAL QUALITY ASSURANCE PROGRAM.—The term 'medical quality assurance program' means any activity carried out on or after the date of enactment of this section by the Department to assess the quality of medical care, including activities conducted by individuals, committees, or other review bodies responsible for quality assurance, credentials, infection control, incident reporting, the delivery, advisement, and support of direct patient care and assessment (including treatment procedures, blood, drugs, and therapeutics), medical records, health resources management review, or identification and prevention of medical, mental health, or dental incidents and risks.

''(3) MEDICAL QUALITY ASSURANCE RECORD OF THE DEPARTMENT.—The term 'medical quality assurance record of the Department' means the proceedings, records (including patient records that the Department creates and maintains as part of a system of records), minutes, and reports that—

''(A) emanate from quality assurance program activities described in paragraph (2); and

''(B) are produced or compiled by the Department as part of a medical quality assurance program.

''(b) CONFIDENTIALITY OF RECORDS.—A medical quality assurance record of the Department that is created as part of a medical quality assurance program—

''(1) is confidential and privileged; and

''(2) except as provided in subsection (d), may not be disclosed to any person or entity.

''(c) PROHIBITION ON DISCLOSURE AND TESTIMONY.—Except as otherwise provided in this section—

''(1) no part of any medical quality assurance record of the Department may be subject to discovery or admitted into evidence in any judicial or administrative proceeding; and

''(2) an individual who reviews or creates a medical quality assurance record of the Department or who participates in any proceeding that reviews or creates a medical quality assurance record of the Department may not be permitted or required to testify in any judicial or administrative proceeding with respect to such record or with respect to any finding, recommendation, evaluation, opinion, or action taken by such individual in connection with such record.

''(d) AUTHORIZED DISCLOSURE AND TESTIMONY.—

''(1) IN GENERAL.—Subject to paragraph (2), a medical quality assurance record of the Department may be disclosed, and a person described in subsection (c)(2) may give testimony in connection with the record, only as follows:

''(A) To a Federal agency or private organization, if such medical quality assurance record of the Department or testimony is needed by the Federal agency or private organization to—

''(i) perform licensing or accreditation functions related to Department health care facilities, a facility affiliated with the Department, or any other location authorized by the Secretary for the performance of health care services; or

''(ii) perform monitoring, required by law, of Department health care facilities, a facility affiliated with the Department, or any other location authorized by the Secretary for the performance of health care services.

''(B) To an administrative or judicial proceeding concerning an adverse action related to the credentialing of or health care provided by a present or former health care provider by the Department.

''(C) To a governmental board or agency or to a professional health care society or organization, if such medical quality assurance record of the Department or testimony is needed by the board, agency, society, or organization to perform licensing, credentialing, or the monitoring of professional standards with respect to any health care provider who is or was a health care provider for the Department.

''(D) To a hospital, medical center, or other institution that provides health care services, if such medical quality assurance record of the Department or testimony is needed by such institution to assess the professional qualifications of any health care provider who is or was a health care provider for the Department and who has applied for or been granted authority or employment to provide health care services in or on behalf of the institution.

''(E) To an employee, a detailee, or a contractor of the Department who has a need for such medical quality assurance record of the Department or testimony to perform official duties or duties within the scope of their employment or contract.

''(F) To a criminal or civil law enforcement agency or instrumentality charged under applicable law with the protection of the public health or safety, if a qualified representative of the agency or instrumentality makes a written request that such medical quality assurance record of the Department or testimony be provided for a purpose authorized by law.

''(G) In an administrative or judicial proceeding commenced by a criminal or civil law enforcement agency or instrumentality described in subparagraph (F), but only with respect to the subject of the proceeding.

''(2) PERSONALLY IDENTIFIABLE INFORMATION.—

''(A) IN GENERAL.—With the exception of the subject of a quality assurance action, personally identifiable information of any person receiving health care services from the Department or of any other person associated with the Department for purposes of a medical quality assurance program that is disclosed in a medical quality assurance record of the Department shall be deleted from that record before any disclosure of the record is made outside the Department.

''(B) APPLICATION.—The requirement under subparagraph (A) shall not apply to the release of information that is permissible under section 552a of title 5, United States Code (commonly known as the 'Privacy Act of 1974').

''(e) DISCLOSURE FOR CERTAIN PURPOSES.—Nothing in this section shall be construed—

''(1) to authorize or require the withholding from any person or entity de-identified aggregate statistical information regarding the results of medical quality assurance programs, under de-identification standards developed by the Secretary in consultation with the Secretary of Health and Human Services, as appropriate, that is released in a manner in accordance with all other applicable legal requirements; or

''(2) to authorize the withholding of any medical quality assurance record of the Department from a committee of either House of Congress, any joint committee of Congress, or the Comptroller General of the United States if the record pertains to any matter within their respective jurisdictions.

''(f) PROHIBITION ON DISCLOSURE OF INFORMATION, RECORDS, OR TESTIMONY.—A person or entity having possession of or access to a medical quality assurance record of the Department or testimony described in this section may not disclose the contents of the record or testimony in any manner or for any purpose except as provided in this section.

''(g) EXEMPTION FROM FREEDOM OF INFORMATION ACT.—A medical quality assurance record of the Department shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code.

''(h) LIMITATION ON CIVIL LIABILITY.—A person who participates in the review or creation of, or provides information to a person or body that reviews or creates, a medical quality assurance record of the Department shall not be civilly liable under this section for that participation or for providing that information if the participation or provision of information was—

''(1) provided in good faith based on prevailing professional standards at the time the medical quality assurance program activity took place; and

''(2) made in accordance with any other applicable legal requirement, including Federal privacy laws and regulations.

''(i) APPLICATION TO INFORMATION IN CERTAIN OTHER RECORDS.—Nothing in this section shall be construed as limiting access to the information in a record created and maintained outside a medical quality assurance program, including the medical record of a patient, on the grounds that the information was presented during meetings of a review body that are part of a medical quality assurance program.

''(j) PENALTY.—Any person who willfully discloses a medical quality assurance record of the Department other than as provided in this section, knowing that the record is a medical quality assurance record of the Department shall be fined not more than $3,000 in the case of a first offense and not more than $20,000 in the case of a subsequent offense.

''(k) RELATIONSHIP TO COAST GUARD.—The requirements of this section shall not apply to any medical quality assurance record of the Department that is created by or for the Coast Guard as part of a medical quality assurance program.

''(l) CONTINUED PROTECTION.—Disclosure under subsection (d) does not permit redisclosure except to the extent the further disclosure is authorized under subsection (d) or is otherwise authorized to be disclosed under this section.

''(m) RELATIONSHIP TO OTHER LAW.—This section shall continue in force and effect, except as otherwise specifically provided in any Federal law enacted after the date of enactment of this Act.

''(n) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to supersede the requirements of—

''(1) the Health Insurance Portability and Accountability Act of 1996 (Public Law 104–191; 110 Stat. 1936) and its implementing regulations;

''(2) part 1 of subtitle D of title XIII of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq.) and its implementing regulations; or

''(3) sections 921 through 926 of the Public Health Service Act (42 U.S.C. 299b–21 through 299b–26) and their implementing regulations.''.

SEC. 6126. TECHNICAL AND CONFORMING AMENDMENTS.

The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

(1) in the table of contents in section 1(b) (Public Law 107–296; 116 Stat. 2135)—

(A) by striking the items relating to sections 528 and 529 and inserting the following:

''Sec. 528. Transfer of equipment during a public health emergency.'';

(B) by striking the items relating to sections 710, 711, 712, and 713 and inserting the following:

''Sec. 710. Employee engagement.
''Sec. 711. Annual employee award program.
''Sec. 712. Acquisition professional career program.'';

(C) by inserting after the item relating to section 1928 the following:

''Sec. 1929. Accountability.'';

(D) by striking the items relating to subtitle C of title XIX and sections 1931 and 1932; and

(E) by adding at the end the following:

''TITLE XXIII—OFFICE OF HEALTH SECURITY

''Sec. 2301. Office of Health Security.
''Sec. 2302. Workforce health and safety.
''Sec. 2303. Coordination of Department of Homeland Security efforts related to food, agriculture, and veterinary defense against terrorism.
''Sec. 2304. Medical countermeasures.
''Sec. 2305. Rules of construction.
''Sec. 2306. Confidentiality of medical quality assurance records.'';

(2) by redesignating section 529 (6 U.S.C. 321r) as section 528;

(3) in section 704(e)(4) (6 U.S.C. 344(e)(4)), by striking ''section 711(a)'' and inserting ''section 710(a))'';

(4) by redesignating sections 711, 712, and 713 as sections 710, 711, and 712, respectively;

(5) in section subsection (d)(3) of section 1923(d)(3) (6 U.S.C. 592), as so redesignated—

(A) in the paragraph heading, by striking ''HAWAIIAN NATIVE-SERVING'' and inserting ''NATIVE HAWAIIAN-SERVING''; and

(B) by striking ''Hawaiian native-serving'' and inserting '' 'Native Hawaiian-serving'';

and

(6) by striking the subtitle heading for subtitle C of title XIX.

Subtitle D—National Cybersecurity Awareness Act

SEC. 6131. SHORT TITLE.

This subtitle may be cited as the ''National Cybersecurity Awareness Act''.

SEC. 6132. FINDINGS.

Congress finds the following:

(1) The presence of ubiquitous internet-connected devices in the everyday lives of citizens of the United States has created opportunities for constant connection and modernization.

(2) A connected society is subject to cybersecurity threats that can compromise even the most personal and sensitive of information.

(3) Connected critical infrastructure is subject to cybersecurity threats that can compromise fundamental economic, health, and safety functions.

(4) The Government of the United States plays an important role in safeguarding the nation from malicious cyber activity.

(5) A citizenry that is knowledgeable regarding cybersecurity is critical to building a robust cybersecurity posture and reducing the threat of cyber attackers stealing sensitive information and causing public harm.

(6) While Cybersecurity Awareness Month is critical to supporting national cybersecurity awareness, it cannot be a once-a-year activity, and there must be a sustained, constant effort to raise awareness about cyber hygiene, encourage individuals in the United States to learn cyber skills, and communicate the ways that cyber skills and careers in cyber advance individual and societal security, privacy, safety, and well-being.

SEC. 6133. CYBERSECURITY AWARENESS.

(a) IN GENERAL.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.), as amended by section 6113(a), is amended by adding at the end the following:

''SEC. 2220H. CYBERSECURITY AWARENESS CAMPAIGNS.

''(a) DEFINITION.—In this section, the term 'Campaign Program' means the campaign program established under subsection (b)(1).

''(b) AWARENESS CAMPAIGN PROGRAM.—

''(1) IN GENERAL.—Not later than 90 days after the date of enactment of the National Cybersecurity Awareness Act, the Director, in coordination with appropriate Federal agencies, shall establish a program for planning and coordinating Federal cybersecurity awareness campaigns.

''(2) ACTIVITIES.—In carrying out the Campaign Program, the Director shall—

''(A) inform non-Federal entities of voluntary cyber hygiene best practices, including information on how to—

''(i) prevent cyberattacks; and

''(ii) mitigate cybersecurity risks; and

''(B) consult with private sector entities, State, local, Tribal, and territorial governments, academia, nonprofit organizations, and civil society—

''(i) to promote cyber hygiene best practices and the importance of cyber skills, including by focusing on tactics that are cost effective and result in significant cybersecurity improvement, such as—

''(I) maintaining strong passwords and the use of password managers;

''(II) enabling multi-factor authentication, including phishing-resistant multi-factor authentication;

''(III) regularly installing software updates;

''(IV) using caution with email attachments and website links; and

''(V) other cyber hygienic considerations, as appropriate;

''(ii) to promote awareness of cybersecurity risks and mitigation with respect to malicious applications on internet-connected devices, including applications to control those devices or use devices for unauthorized surveillance of users;

''(iii) to help consumers identify products that are designed to support user and product security, such as products designed using the Secure-by-Design and Secure-by-Default principles of the Agency or the Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products of the National Institute of Standards and Technology, published February 4, 2022 (or any subsequent version);

''(iv) to coordinate with other Federal agencies, as determined appropriate by the Director, to—

''(I) develop and promote relevant cybersecurity-related and cyber skills-related awareness activities and resources; and

''(II) ensure the Federal Government is coordinated in communicating accurate and timely cybersecurity information;

''(v) to expand nontraditional outreach mechanisms to ensure that entities, including low-income and rural communities, small and medium sized businesses and institutions, and State, local, Tribal, and territorial partners, receive cybersecurity awareness outreach in an equitable manner; and

''(vi) to encourage participation in cyber workforce development ecosystems and to expand adoption of best practices to grow the national cyber workforce.

''(3) REPORTING.—

''(A) IN GENERAL.—Not later than 180 days after the date of enactment of the National Cybersecurity Awareness Act, and annually thereafter, the Director, in consultation with the heads of appropriate Federal agencies, shall submit to the appropriate congressional committees a report regarding the Campaign Program.

''(B) CONTENTS.—Each report submitted pursuant to subparagraph (A) shall include—

''(i) a summary of the activities of the Agency that support promoting cybersecurity awareness under the Campaign Program, including consultations made under paragraph (2)(B);

''(ii) an assessment of the effectiveness of techniques and methods used to promote national cybersecurity awareness under the Campaign Program; and

''(iii) recommendations on how to best promote cybersecurity awareness nationally.

''(c) CYBERSECURITY CAMPAIGN RESOURCES.—

''(1) IN GENERAL.—Not later than 180 days after the date of enactment of the National Cybersecurity Awareness Act, the Director shall develop and maintain a repository for the resources, tools, and public communications of the Agency that promote cybersecurity awareness.

''(2) REQUIREMENTS.—The resources described in paragraph (1) shall be—

''(A) made publicly available online; and

''(B) regularly updated to ensure the public has access to relevant and timely cybersecurity awareness information.''.

(b) RESPONSIBILITIES OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.—Section 2202(c) of the Homeland Security Act of 2002 (6 U.S.C. 652(c)) is amended—

(1) in paragraph (13), by striking ''; and'' and inserting a semicolon;

(2) by redesignating paragraph (14) as paragraph (16); and

(3) by inserting after paragraph (13) the following:

''(14) lead and coordinate Federal efforts to promote national cybersecurity awareness;''.

(c) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135), as amended by section 6113(b), is amended by inserting after the item relating to section 2220G the following:

''Sec. 2220H. Cybersecurity awareness campaigns.''.

Subtitle E—DHS International Cyber Partner Act of 2023

SEC. 6141. SHORT TITLE.

This subtitle may be cited as the ''DHS International Cyber Partner Act of 2023''.

SEC. 6142. PURPOSE.

The purposes of this subtitle are to—

(1) authorize the Secretary of Homeland Security to assign personnel to foreign locations to support the missions of the Department of Homeland Security; and

(2) provide assistance and expertise to foreign governments, international organizations, and international entities on cybersecurity and infrastructure security.

SEC. 6143. INTERNATIONAL ASSIGNMENT AND ASSISTANCE.

(a) IN GENERAL.—Title I of the Homeland Security Act of 2002 (6 U.S.C. 111 et seq.) is amended by adding at the end the following:

''SEC. 104. INTERNATIONAL ASSIGNMENT AND ASSISTANCE.

''(a) INTERNATIONAL ASSIGNMENT.—

''(1) IN GENERAL.—The Secretary, with the concurrence of the Secretary of State, may assign personnel of the Department to a duty station that is located outside the United States at which the Secretary determines representation of the Department is necessary to accomplish the cybersecurity and infrastructure security missions of the Department and to carry out duties and activities as assigned by the Secretary.

''(2) CONCURRENCE ON ACTIVITIES.—The activities of personnel of the Department who are assigned under this subsection shall be—

''(A) performed with the concurrence of the chief of mission to the foreign country to which such personnel are assigned; and

''(B) consistent with the duties and powers of the Secretary of State and the chief of mission for a foreign country under section 103 of the Omnibus Diplomatic Security and Antiterrorism Act of 1986 (22 U.S.C. 4802) and section 207 of the Foreign Service Act of 1980 (22 U.S.C. 3927), respectively.

''(b) INTERNATIONAL SUPPORT.—

''(1) IN GENERAL.—If the Secretary makes a determination described in paragraph (2), the Secretary, with the concurrence of the Secretary of State, may provide equipment, services, technical assistance, or expertise on cybersecurity, infrastructure security, and resilience to a foreign government, an international organization, or an international entity, with or without reimbursement, including, as appropriate—

''(A) cybersecurity and infrastructure security advice, training, capacity development, education, best practices, incident response, threat hunting, and other similar capabilities;

''(B) sharing and exchanging cybersecurity and infrastructure security information, including research and development, threat indicators, risk assessments, strategies, and security recommendations;

''(C) cybersecurity and infrastructure security test and evaluation support and services;

''(D) cybersecurity and infrastructure security research and development support and services; and

''(E) any other assistance that the Secretary prescribes.

''(2) DETERMINATION.—A determination described in this paragraph is a determination by the Secretary that providing equipment, services, technical assistance, or expertise under paragraph (1) would—

''(A) further the homeland security interests of the United States; and

''(B) enhance the ability of a foreign government, an international organization, or an international entity to work cooperatively with the United States to advance the homeland security interests of the United States.

''(3) LIMITATIONS.—Any equipment provided under paragraph (1)—

''(A) may not include offensive security capabilities; and

''(B) shall be limited to enabling defensive cybersecurity and infrastructure security activities by the receiving entity, such as cybersecurity tools or explosive detection and mitigation equipment.

''(4) REIMBURSEMENT OF EXPENSES.—If the Secretary determines that collection of payment is appropriate, the Secretary is authorized to collect payment from the receiving entity for the cost of equipment, services, technical assistance, and expertise provided under paragraph (1) and any accompanying shipping costs.

''(5) RECEIPTS CREDITED AS OFFSETTING COLLECTIONS.—Notwithstanding section 3302 of title 31, United States Code, any amount collected under paragraph (4)—

''(A) shall be credited as offsetting collections to the account that finances the equipment, services, technical assistance, or expertise for which the payment is received; and

''(B) shall remain available until expended for the purpose of providing for the security interests of the homeland.

''(c) RULE OF CONSTRUCTION.—This section shall not be construed to affect, augment, or diminish the authority of the Secretary of State.

''(d) CONGRESSIONAL REPORTING AND NOTIFICATION.—

''(1) REPORT ON ASSISTANCE.—Not later than 1 year after the date of enactment of the DHS International Cyber Partner Act of 2023, and every year thereafter, the Secretary shall provide 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 includes, for each instance in which assistance is provided under subsection (b)—

''(A) the foreign government, international organization, or international entity provided the assistance;

''(B) the reason for providing the assistance;

''(C) the equipment, services, technical assistance, or expertise provided; and

''(D) whether the equipment, services, technical assistance, or expertise was provided on a reimbursable or nonreimbursable basis, and the rational for why the assistance was provided with or without reimbursement.

''(2) COPIES OF AGREEMENTS.—Not later than 30 days after the effective date, under the authority under subsection (b), of a contract, memorandum, or agreement with a foreign government, international organization, or international entity to provide assistance, the Secretary shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a copy of the contract, memorandum, or agreement.

''(3) NOTICE ON ASSIGNMENTS.—Not later than 30 days after assigning personnel to a duty station located outside the United States in accordance with subsection (a)(1), the Secretary shall notify the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives regarding the assignment.''.

(b) CONFORMING AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–196; 116 Stat. 2135) is amended by inserting after the item relating to section 103 the following:

''Sec. 104. International assignment and assistance.''.

SEC. 6144. CISA ACTIVITIES.

(a) DIRECTOR.—Section 2202(c) of the Homeland Security Act of 2002 (6 U.S.C. 652(c)), as amended by section 6133(b), is amended by inserting after paragraph (14) the following:

''(15) provide support for the cybersecurity and physical security of critical infrastructure of international partners and allies in furtherance of the homeland security interests of the United States, which may include, consistent with section 104, assigning personnel to a duty station that is located outside the United States and providing equipment, services, technical assistance, or expertise; and''.

(b) FOREIGN LOCATIONS.—Section 2202(g)(1) of the Homeland Security Act of 2002 (6 U.S.C. 652(g)(1)) is amended by inserting '', including locations outside the United States'' before the period at the end.

(c) CYBER PLANNING.—Section 2216 of the Homeland Security Act of 2002 (6 U.S.C. 665b) is amended—

(1) in subsection (a), in the first sentence, by inserting '', including international partners, as appropriate'' after ''for public and private sector entities''; and

(2) in subsection (c)(2)—

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

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

(C) by adding at the end the following

''(G) for planning with international partners, the Department of State.''.

SEC. 6145. LIMITATIONS.

Under the authority provided under this subtitle, or an amendment made by this subtitle, the Secretary of Homeland Security may not—

(1) engage in any activity that would censor a citizen of the United States;

(2) conduct surveillance of a citizen of the United States; or

(3) interfere with an election in the United States.

TITLE LXII—CYBERSECURITY AND DIGITAL IDENTITY VERIFICATION

Subtitle A—Satellite Cybersecurity Act

SEC. 6201. SHORT TITLE.

This subtitle may be cited as the ''Satellite Cybersecurity Act''.

SEC. 6202. DEFINITIONS.

In this subtitle:

(1) CLEARINGHOUSE.—The term ''clearinghouse'' means the commercial satellite system cybersecurity clearinghouse required to be developed and maintained under section 6204(b)(1).

(2) COMMERCIAL SATELLITE SYSTEM.—The term ''commercial satellite system''—

(A) means a system that—

(i) is owned or operated by a non-Federal entity based in the United States; and

(ii) is composed of not less than 1 earth satellite; and

(B) includes—

(i) any ground support infrastructure for each satellite in the system; and

(ii) any transmission link among and between any satellite in the system and any ground support infrastructure in the system.

(3) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' has the meaning given the term in subsection (e) of the Critical Infrastructure Protection Act of 2001 (42 U.S.C. 5195c).

(4) CYBERSECURITY RISK.—The term ''cybersecurity risk'' has the meaning given the term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

(5) CYBERSECURITY THREAT.—The term ''cybersecurity threat'' has the meaning given the term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

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

(7) SECTOR RISK MANAGEMENT AGENCY.—The term ''sector risk management agency'' has the meaning given the term ''Sector Risk Management Agency'' in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

SEC. 6203. REPORT ON COMMERCIAL SATELLITE CYBERSECURITY.

(a) STUDY.—The Comptroller General of the United States shall conduct a study on the actions the Federal Government has taken to support the cybersecurity of commercial satellite systems, including as part of any action to address the cybersecurity of critical infrastructure sectors.

(b) REPORT.—Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall report to the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security and the Committee on Science, Space, and Technology of the House of Representatives on the study conducted under subsection (a), which shall include information—

(1) on efforts of the Federal Government, and the effectiveness of those efforts, to—

(A) address or improve the cybersecurity of commercial satellite systems; and

(B) support related efforts with international entities or the private sector;

(2) on the resources made available to the public by Federal agencies to address cybersecurity risks and threats to commercial satellite systems, including resources made available through the clearinghouse;

(3) on the extent to which commercial satellite systems are reliant on, or relied on by, critical infrastructure;

(4) that includes an analysis of how commercial satellite systems and the threats to those systems are integrated into Federal and non-Federal critical infrastructure risk analyses and protection plans;

(5) on the extent to which Federal agencies are reliant on commercial satellite systems and how Federal agencies mitigate cybersecurity risks associated with those systems;

(6) on the extent to which Federal agencies are reliant on commercial satellite systems that are owned wholly or in part or controlled by foreign entities, or that have infrastructure in foreign countries, and how Federal agencies mitigate associated cybersecurity risks;

(7) on the extent to which Federal agencies coordinate or duplicate authorities and take other actions focused on the cybersecurity of commercial satellite systems; and

(8) as determined appropriate by the Comptroller General of the United States, that includes recommendations for further Federal action to support the cybersecurity of commercial satellite systems, including recommendations on information that should be shared through the clearinghouse.

(c) CONSULTATION.—In carrying out subsections (a) and (b), the Comptroller General of the United States shall coordinate with appropriate Federal agencies and organizations, including—

(1) the Office of the National Cyber Director;

(2) the Department of Homeland Security;

(3) the Department of Commerce;

(4) the Department of Defense;

(5) the Department of Transportation;

(6) the Federal Communications Commission;

(7) the National Aeronautics and Space Administration;

(8) the National Executive Committee for Space-Based Positioning, Navigation, and Timing; and

(9) the National Space Council.

(d) BRIEFING.—Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall provide a briefing to the appropriate congressional committees on the study conducted under subsection (a).

(e) CLASSIFICATION.—The report made under subsection (b) shall be unclassified but may include a classified annex.

SEC. 6204. RESPONSIBILITIES OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

(a) SMALL BUSINESS CONCERN DEFINED.—In this section, the term ''small business concern'' has the meaning given the term in section 3 of the Small Business Act (15 U.S.C. 632).

(b) ESTABLISHMENT OF COMMERCIAL SATELLITE SYSTEM CYBERSECURITY CLEARINGHOUSE.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Director shall develop and maintain a commercial satellite system cybersecurity clearinghouse.

(2) REQUIREMENTS.—The clearinghouse—

(A) shall be publicly available online;

(B) shall contain publicly available commercial satellite system cybersecurity resources, including the voluntary recommendations consolidated under subsection (c)(1);

(C) shall contain appropriate materials for reference by entities that develop, operate, or maintain commercial satellite systems;

(D) shall contain materials specifically aimed at assisting small business concerns with the secure development, operation, and maintenance of commercial satellite systems; and

(E) may contain controlled unclassified information distributed to commercial entities through a process determined appropriate by the Director.

(3) CONTENT MAINTENANCE.—The Director shall maintain current and relevant cybersecurity information on the clearinghouse.

(4) EXISTING PLATFORM OR WEBSITE.—To the extent practicable, the Director shall establish and maintain the clearinghouse using an online platform, a website, or a capability in existence as of the date of enactment of this Act.

(c) CONSOLIDATION OF COMMERCIAL SATELLITE SYSTEM CYBERSECURITY RECOMMENDATIONS.—

(1) IN GENERAL.—The Director shall consolidate voluntary cybersecurity recommendations designed to assist in the development, maintenance, and operation of commercial satellite systems.

(2) REQUIREMENTS.—The recommendations consolidated under paragraph (1) shall include materials appropriate for a public resource addressing, to the greatest extent practicable, the following:

(A) Risk-based, cybersecurity-informed engineering, including continuous monitoring and resiliency.

(B) Planning for retention or recovery of positive control of commercial satellite systems in the event of a cybersecurity incident.

(C) Protection against unauthorized access to vital commercial satellite system functions.

(D) Physical protection measures designed to reduce the vulnerabilities of a commercial satellite system's command, control, and telemetry receiver systems.

(E) Protection against jamming, eavesdropping, hijacking, computer network exploitation, spoofing, threats to optical satellite communications, and electromagnetic pulse.

(F) Security against threats throughout a commercial satellite system's mission lifetime.

(G) Management of supply chain risks that affect the cybersecurity of commercial satellite systems.

(H) Protection against vulnerabilities posed by ownership of commercial satellite systems or commercial satellite system companies by foreign entities.

(I) Protection against vulnerabilities posed by locating physical infrastructure, such as satellite ground control systems, in foreign countries.

(J) As appropriate, and as applicable pursuant to the maintenance requirement under subsection (b)(3), relevant findings and recommendations from the study conducted by the Comptroller General of the United States under section 6203(a).

(K) Any other recommendations to ensure the confidentiality, availability, and integrity of data residing on or in transit through commercial satellite systems.

(d) IMPLEMENTATION.—In implementing this section, the Director shall—

(1) to the extent practicable, carry out the implementation in partnership with the private sector;

(2) coordinate with—

(A) the Office of the National Cyber Director, the National Space Council, and the

head of any other agency determined appropriate by the Office of the National Cyber Director or the National Space Council; and

(B) the heads of appropriate Federal agencies with expertise and experience in satellite operations, including the entities described in section 6203(c), to enable—

(i) the alignment of Federal efforts on commercial satellite system cybersecurity; and

(ii) to the extent practicable, consistency in Federal recommendations relating to commercial satellite system cybersecurity; and

(3) consult with non-Federal entities developing commercial satellite systems or otherwise supporting the cybersecurity of commercial satellite systems, including private, consensus organizations that develop relevant standards.

(e) REPORT.—Not later than 1 year after the date of enactment of this Act, and every 2 years thereafter until the date that is 9 years after the date of enactment of this Act, the Director shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security and the Committee on Science, Space, and Technology of the House of Representatives a report summarizing—

(1) any partnership with the private sector described in subsection (d)(1);

(2) any consultation with a non-Federal entity described in subsection (d)(3);

(3) the coordination carried out pursuant to subsection (d)(2);

(4) the establishment and maintenance of the clearinghouse pursuant to subsection (b);

(5) the recommendations consolidated pursuant to subsection (c)(1); and

(6) any feedback received by the Director on the clearinghouse from non-Federal entities.

SEC. 6205. STRATEGY.

Not later than 120 days after the date of the enactment of this Act, the National Space Council, jointly with the Office of the National Cyber Director, in coordination with the Director of the Office of Space Commerce and the heads of other relevant agencies, shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security and the Committee on Science, Space, and Technology of the House of Representatives a strategy for the activities of Federal agencies to address and improve the cybersecurity of commercial satellite systems, which shall include an identification of—

(1) proposed roles and responsibilities for relevant agencies; and

(2) as applicable, the extent to which cybersecurity threats to such systems are addressed in Federal and non-Federal critical infrastructure risk analyses and protection plans.

SEC. 6206. RULES OF CONSTRUCTION.

Nothing in this subtitle shall be construed to—

(1) designate commercial satellite systems or other space assets as a critical infrastructure sector; or

(2) infringe upon or alter the authorities of the agencies described in section 6203(c).

SEC. 6207. SECTOR RISK MANAGEMENT AGENCY TRANSFER.

If the President designates an infrastructure sector that includes commercial satellite systems as a critical infrastructure sector pursuant to the process established under section 9002(b)(3) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 652a(b)(3)) and subsequently designates a sector risk management agency for that critical infrastructure sector that is not the Cybersecurity and Infrastructure Security Agency, the President may direct the Director to transfer the authorities of the Director under section 6204 of this subtitle to the head of the designated sector risk management agency.

Subtitle B—Rural Hospital Cybersecurity Enhancement Act

SEC. 6211. SHORT TITLE.

This subtitle may be cited as the ''Rural Hospital Cybersecurity Enhancement Act''.

SEC. 6212. DEFINITIONS.

In this subtitle:

(1) AGENCY.—The term ''agency'' has the meaning given the term in section 551 of title 5, United States Code.

(2) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

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

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

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

(4) GEOGRAPHIC DIVISION.—The term ''geographic division'' means a geographic division that is among the 9 geographic divisions determined by the Bureau of the Census.

(5) RURAL HOSPITAL.—The term ''rural hospital'' means a healthcare facility that—

(A) is located in a non-urbanized area, as determined by the Bureau of the Census; and

(B) provides inpatient and outpatient healthcare services, including primary care, emergency care, and diagnostic services.

(6) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

SEC. 6213. RURAL HOSPITAL CYBERSECURITY WORKFORCE DEVELOPMENT STRATEGY.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Secretary, acting through the Director, shall develop and transmit to the appropriate committees of Congress a comprehensive rural hospital cybersecurity workforce development strategy to address the growing need for skilled cybersecurity professionals in rural hospitals.

(b) CONSULTATION.—

(1) AGENCIES.—In carrying out subsection (a), the Secretary and Director may consult with the Secretary of Health and Human Services, the Secretary of Education, the Secretary of Labor, and any other appropriate head of an agency.

(2) PROVIDERS.—In carrying out subsection (a), the Secretary shall consult with not less than 2 representatives of rural healthcare providers from each geographic division in the United States.

(c) CONSIDERATIONS.—The rural hospital cybersecurity workforce development strategy developed under subsection (a) shall, at a minimum, consider the following components:

(1) Partnerships between rural hospitals, non-rural healthcare systems, educational institutions, private sector entities, and nonprofit organizations to develop, promote, and expand the rural hospital cybersecurity workforce, including through education and training programs tailored to the needs of rural hospitals.

(2) The development of a cybersecurity curriculum and teaching resources that focus on teaching technical skills and abilities related to cybersecurity in rural hospitals for use in community colleges, vocational schools, and other educational institutions located in rural areas.

(3) Identification of—

(A) cybersecurity workforce challenges that are specific to rural hospitals, as well as challenges that are relative to hospitals generally; and

(B) common practices to mitigate both sets of challenges described in subparagraph (A).

(4) Recommendations for legislation, rulemaking, or guidance to implement the components of the rural hospital cybersecurity workforce development strategy.

(d) ANNUAL BRIEFING.—Not later than 60 days after the date on which the first full fiscal year ends following the date on which the Secretary transmits the rural hospital cybersecurity workforce development strategy developed under subsection (a), and not later than 60 days after the date on which each fiscal year thereafter ends, the Secretary shall provide a briefing to the appropriate committees of Congress that includes, at a minimum, information relating to—

(1) updates to the rural hospital cybersecurity workforce development strategy, as appropriate;

(2) any programs or initiatives established pursuant to the rural hospital cybersecurity workforce development strategy, as well as the number of individuals trained or educated through such programs or initiatives;

(3) additional recommendations for legislation, rulemaking, or guidance to implement the components of the rural hospital cybersecurity workforce development strategy; and

(4) the effectiveness of the rural hospital cybersecurity workforce development strategy in addressing the need for skilled cybersecurity professionals in rural hospitals.

SEC. 6214. INSTRUCTIONAL MATERIALS FOR RURAL HOSPITALS.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Director shall make available instructional materials for rural hospitals that can be used to train staff on fundamental cybersecurity efforts.

(b) DUTIES.—In carrying out subsection (a), the Director shall—

(1) consult with appropriate heads of agencies, experts in cybersecurity education, and rural healthcare experts;

(2) identify existing cybersecurity instructional materials that can be adapted for use in rural hospitals and create new materials as needed; and

(3) conduct an awareness campaign to promote the materials available to rural hospitals developed under subsection (a).

SEC. 6215. NO ADDITIONAL FUNDS.

No additional funds are authorized to be appropriated for the purpose of carrying out this subtitle.

TITLE LXIII—U.S. CUSTOMS AND BORDER PROTECTION

Subtitle A—Non-Intrusive Inspection Expansion

SEC. 6301. SHORT TITLE.

This subtitle may be cited as the ''Non-Intrusive Inspection Expansion Act''.

SEC. 6302. USE OF NON-INTRUSIVE INSPECTION SYSTEMS AT LAND PORTS OF ENTRY.

(a) FISCAL YEAR 2026.—Using non-intrusive inspection systems acquired through previous appropriations Acts, beginning not later than September 30, 2026, U.S. Customs and Border Protection shall use non-intrusive inspection systems at land ports of entry to scan, cumulatively, at ports of entry where systems are in place by the deadline, not fewer than—

(1) 40 percent of passenger vehicles entering the United States; and

(2) 90 percent of commercial vehicles entering the United States.

(b) SUBSEQUENT FISCAL YEARS.—Beginning in fiscal year 2027, U.S. Customs and Border

Protection shall use non-intrusive inspection systems at land ports of entry to reach the next projected benchmark for incremental scanning of passenger and commercial vehicles entering the United States at such ports of entry.

(c) BRIEFING.—Not later than May 30, 2026, the Commissioner of U.S. Customs and Border Protection shall brief the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives regarding the progress made during the first half of fiscal year 2026 in achieving the scanning benchmarks described in subsection (a).

(d) REPORT.—If the scanning benchmarks described in subsection (a) are not met by the end of fiscal year 2026, not later than 120 days after the end of that fiscal year, the Commissioner of U.S. Customs and Border Protection shall submit a report to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives that—

(1) analyzes the causes for not meeting such requirements;

(2) identifies any resource gaps and challenges; and

(3) details the steps that will be taken to ensure compliance with such requirements in the subsequent fiscal year.

SEC. 6303. NON-INTRUSIVE INSPECTION SYSTEMS FOR OUTBOUND INSPECTIONS.

(a) STRATEGY.—Not later than 180 days after the date of the enactment of this Act, the Commissioner of U.S. Customs and Border Protection shall submit a strategy to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives for increasing sustained outbound inspection operations at land ports of entry that includes—

(1) the number of existing and planned outbound inspection lanes at each port of entry;

(2) infrastructure limitations that limit the ability of U.S. Customs and Border Protection to deploy non-intrusive inspection systems for outbound inspections;

(3) the number of additional non-intrusive inspection systems that are necessary to increase scanning capacity for outbound inspections; and

(4) plans for funding and acquiring the systems described in paragraph (3).

(b) IMPLEMENTATION.—Beginning not later than September 30, 2026, U.S. Customs and Border Protection shall use non-intrusive inspection systems at land ports of entry to scan not fewer than 10 percent of all vehicles exiting the United States through land ports of entry.

SEC. 6304. GAO REVIEW AND REPORT.

(a) REVIEW.—

(1) IN GENERAL.—The Comptroller General of the United States shall conduct a review of the use by U.S. Customs and Border Protection of non-intrusive inspection systems for border security.

(2) ELEMENTS.—The review required under paragraph (1) shall—

(A) identify—

(i) the number and types of non-intrusive inspection systems deployed by U.S. Customs and Border Protection; and

(ii) the locations to which such systems have been deployed; and

(B) examine the manner in which U.S. Customs and Border Protection—

(i) assesses the effectiveness of such systems; and

(ii) uses such systems in conjunction with other border security resources and assets, such as border barriers and technology, to detect and interdict drug smuggling and trafficking at the southwest border of the United States.

(b) REPORT.—Not later than 2 years after the date of the enactment of this Act, the Comptroller General shall submit a report to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives containing the findings of the review conducted pursuant to subsection (a).

Subtitle B—Enhancing Department of Homeland Security Drug Seizures

SEC. 6311. SHORT TITLE.

This subtitle may be cited as the ''Enhancing DHS Drug Seizures Act''.

SEC. 6312. COORDINATION AND INFORMATION SHARING.

(a) PUBLIC-PRIVATE PARTNERSHIPS.—

(1) STRATEGY.—Not later than 180 days after the date of enactment of this Act, the Secretary of Homeland Security shall develop a strategy to strengthen existing and establish new public-private partnerships with shipping, chemical, and pharmaceutical industries to assist with early detection and interdiction of illicit drugs and precursor chemicals.

(2) CONTENTS.—The strategy required under paragraph (1) shall contain goals and objectives for employees of the Department of Homeland Security to ensure the tactics, techniques, and procedures gained from the public-private partnerships described in paragraph (1) are included in policies, best practices, and training for the Department.

(3) IMPLEMENTATION PLAN.—Not later than 180 days after developing the strategy required under paragraph (1), the Secretary of Homeland Security shall develop an implementation plan for the strategy, which shall outline departmental lead and support roles, responsibilities, programs, and timelines for accomplishing the goals and objectives of the strategy.

(4) BRIEFING.—The Secretary of Homeland Security shall provide annual briefings to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives regarding the progress made in addressing the implementation plan developed pursuant to paragraph (3).

(b) ASSESSMENT OF DRUG TASK FORCES.—

(1) IN GENERAL.—The Secretary of Homeland Security shall conduct an assessment of the counterdrug task forces in which the Department of Homeland Security, including components of the Department, participates in or leads, which shall include—

(A) areas of potential overlap;

(B) opportunities for sharing information and best practices;

(C) how the Department's processes for ensuring accountability and transparency in its vetting and oversight of partner agency task force members align with best practices; and

(D) corrective action plans for any capability limitations and deficient or negative findings identified in the report for any such task forces led by the Department.

(2) REPORT.—Not later than 180 days after the date of enactment of this Act, the Secretary of Homeland Security shall submit a report to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives that contains a summary of the results of the assessment conducted pursuant to paragraph (1).

(3) CORRECTIVE ACTION PLAN.—The Secretary of Homeland Security shall—

(A) implement the corrective action plans described in paragraph (1)(D) immediately after the submission of the report pursuant to paragraph (2); and

(B) provide annual briefings to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives regarding the progress made in implementing the corrective action plans.

(c) COMBINATION OF BRIEFINGS.—The Secretary of Homeland Security may combine the briefings required under subsections (a)(4) and (b)(3)(B) and provide such combined briefings through fiscal year 2026.

SEC. 6313. DANGER PAY FOR DEPARTMENT OF HOMELAND SECURITY PERSONNEL DEPLOYED ABROAD.

(a) IN GENERAL.—Subtitle H of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 451 et seq.) is amended by inserting after section 881 the following:

''SEC. 881A. DANGER PAY ALLOWANCE.

''(a) AUTHORIZATION.—An employee of the Department, while stationed in a foreign area, may be granted a danger pay allowance, not to exceed 35 percent of the basic pay of such employee, for any period during which such foreign area experiences a civil insurrection, a civil war, ongoing terrorist acts, or wartime conditions that threaten physical harm or imminent danger to the health or well-being of such employee.

''(b) NOTICE.—Before granting or terminating a danger pay allowance to any employee pursuant to subsection (a), the Secretary, after consultation with the Secretary of State, shall notify the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Foreign Relations of the Senate, the Committee on Homeland Security of the House of Representatives, and the Committee on Foreign Affairs of the House of Representatives of—

''(1) the intent to make such payments and the circumstances justifying such payments; or

''(2) the intent to terminate such payments and the circumstances justifying such termination.''.

SEC. 6314. IMPROVING TRAINING TO FOREIGN-VETTED LAW ENFORCEMENT OR NATIONAL SECURITY UNITS.

The Secretary of Homeland Security, or the designee of the Secretary, may waive reimbursement for salary expenses of Department of Homeland Security for personnel providing training to foreign-vetted law enforcement or national security units in accordance with an agreement with the Department of Defense pursuant to section 1535 of title 31, United States Code.

SEC. 6315. ENHANCING THE OPERATIONS OF U.S. CUSTOMS AND BORDER PROTECTION IN FOREIGN COUNTRIES.

Section 411(f) of the Homeland Security Act of 2002 (6 U.S.C. 211(f)) is amended—

(1) by redesignating paragraph (4) as paragraph (5); and

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

''(4) PERMISSIBLE ACTIVITIES.—

''(A) IN GENERAL.—Employees of U.S. Customs and Border Protection and other customs officers designated in accordance with the authorities granted to officers and agents of Air and Marine Operations may provide the support described in subparagraph (B) to authorities of the government of a foreign country, including by conducting joint operations with appropriate government officials within the territory of such country, if an arrangement has been entered into between the Government of the United States and the government of such country that permits such support by such employees and officers.

''(B) SUPPORT DESCRIBED.—The support described in this subparagraph is support for—

''(i) the monitoring, locating, tracking, and deterrence of—

''(I) illegal drugs to the United States;

''(II) the illicit smuggling of persons and goods into the United States;

''(III) terrorist threats to the United States; and

''(IV) other threats to the security or economy of the United States;

''(ii) emergency humanitarian efforts; and

''(iii) law enforcement capacity-building efforts.

''(C) PAYMENT OF CLAIMS.—

''(i) IN GENERAL.—Subject to clauses (ii) and (iv), the Secretary may expend funds that have been appropriated or otherwise made available for the operating expenses of the Department to pay claims for money damages against the United States, in accordance with the first paragraph of section 2672 of title 28, United States Code, which arise in a foreign country in connection with U.S. Customs and Border Protection operations in such country.

''(ii) SUBMISSION DEADLINE.—A claim may be allowed under clause (i) only if it is presented not later than 2 years after it accrues.

''(iii) REPORT.—Not later than 90 days after the date on which the expenditure authority under clause (i) expires pursuant to clause (iv), the Secretary shall submit a report to Congress that describes, for each of the payments made pursuant to clause (i)—

''(I) the foreign entity that received such payment;

''(II) the amount paid to such foreign entity;

''(III) the country in which such foreign entity resides or has its principal place of business; and

''(IV) a detailed account of the circumstances justify such payment.

''(iv) SUNSET.—The expenditure authority under clause (i) shall expire on the date that is 5 years after the date of the enactment of the Enhancing DHS Drug Seizures Act.''.

SEC. 6316. DRUG SEIZURE DATA IMPROVEMENT.

(a) STUDY.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall conduct a study to identify any opportunities for improving drug seizure data collection.

(b) ELEMENTS.—The study required under subsection (a) shall—

(1) include a survey of the entities that use drug seizure data; and

(2) address—

(A) any additional data fields or drug type categories that should be added to U.S. Customs and Border Protection's SEACATS, U.S. Border Patrol's e3 portal, and any other systems deemed appropriate by the Commissioner of U.S. Customs and Border Protection, in accordance with the first recommendation in the Government Accountability Office's report GAO-22-104725, entitled ''Border Security: CBP Could Improve How It Categorizes Drug Seizure Data and Evaluates Training'';

(B) how all the Department of Homeland Security components that collect drug seizure data can standardize their data collection efforts and deconflict drug seizure reporting;

(C) how the Department of Homeland Security can better identify, collect, and analyze additional data on precursor chemicals, synthetic drugs, novel psychoactive substances, and analogues that have been seized by U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement; and

(D) how the Department of Homeland Security can improve its model of anticipated drug flow into the United States.

(c) IMPLEMENTATION OF FINDINGS.—Following the completion of the study required under subsection (a)—

(1) the Secretary of Homeland Security, in accordance with the Office of National Drug Control Policy's 2022 National Drug Control Strategy, shall modify Department of Homeland Security drug seizure policies and training programs, as appropriate, consistent with the findings of such study; and

(2) the Commissioner of U.S. Customs and Border Protection, in consultation with the Director of U.S. Immigration and Customs Enforcement, shall make any necessary updates to relevant systems to include the results of confirmatory drug testing results.

SEC. 6317. DRUG PERFORMANCE MEASURES.

Not later than 180 days after the date of enactment of this Act, the Secretary of Homeland Security shall develop and implement a plan to ensure that components of the Department of Homeland Security develop and maintain outcome-based performance measures that adequately assess the success of drug interdiction efforts and how to utilize the existing drug-related metrics and performance measures to achieve the missions, goals, and targets of the Department.

SEC. 6318. PENALTIES FOR HINDERING IMMIGRATION, BORDER, AND CUSTOMS CONTROLS.

(a) PERSONNEL AND STRUCTURES.—Title II of the Immigration and Nationality Act (8 U.S.C. 1151 et seq.) is amended by inserting after section 274D the following:

''SECTION 274E. DESTROYING OR EVADING BORDER CONTROLS.

''(a) IN GENERAL.—It shall be unlawful to knowingly and without lawful authorization—

''(1)(A) destroy or significantly damage any fence, barrier, sensor, camera, or other physical or electronic device deployed by the Federal Government to control an international border of, or a port of entry to, the United States; or

''(B) otherwise construct, excavate, or make any structure intended to defeat, circumvent or evade such a fence, barrier, sensor camera, or other physical or electronic device deployed by the Federal Government to control an international border of, or a port of entry to, the United States; and

''(2) in carrying out an act described in paragraph (1), have the intent to knowingly and willfully—

''(A) secure a financial gain;

''(B) further the objectives of a criminal organization; and

''(C) violate—

''(i) section 274(a)(1)(A)(i);

''(ii) the customs and trade laws of the United States (as defined in section 2(4) of the Trade Facilitation and Trade Enforcement Act of 2015 (Public Law 114–125));

''(iii) any other Federal law relating to transporting controlled substances, agriculture, or monetary instruments into the United States; or

''(iv) any Federal law relating to border controls measures of the United States.

''(b) PENALTY.—Any person who violates subsection (a) shall be fined under title 18, United States Code, imprisoned for not more than 5 years, or both.''.

(b) CLERICAL AMENDMENT.—The table of contents for the Immigration and Nationality Act (8 U.S.C. 1101 et seq.) is amended by inserting after the item relating to section 274D the following:

''Sec. 274E. Destroying or evading border controls.''.

TITLE LXIV—MISCELLANEOUS

Subtitle A—Government-wide Study Relating to High-security Leased Space

SEC. 6401. GOVERNMENT-WIDE STUDY.

(a) DEFINITIONS.—In this section:

(1) ADMINISTRATOR.—The term ''Administrator'' means the Administrator of General Services.

(2) BENEFICIAL OWNER.—

(A) IN GENERAL.—The term ''beneficial owner'', with respect to a covered entity, means each natural person who, directly or indirectly, through any contract, arrangement, understanding, relationship, or otherwise—

(i) exercises substantial control over the covered entity; or

(ii) owns or controls not less than 25 percent of the ownership interests of, or receives substantial economic benefits from the assets of, the covered entity.

(B) EXCLUSIONS.—The term ''beneficial owner'', with respect to a covered entity, does not include—

(i) a minor;

(ii) a person acting as a nominee, intermediary, custodian, or agent on behalf of another person;

(iii) a person acting solely as an employee of the covered entity and whose control over or economic benefits from the covered entity derives solely from the employment status of the person;

(iv) a person whose only interest in the covered entity is through a right of inheritance, unless the person also meets the requirements of subparagraph (A); or

(v) a creditor of the covered entity, unless the creditor also meets the requirements of subparagraph (A).

(C) ANTI-ABUSE RULE.—The exclusions under subparagraph (B) shall not apply if, in the determination of the Administrator, an exclusion is used for the purpose of evading, circumventing, or abusing the requirements of this Act.

(3) CONTROL.—The term ''control'', with respect to a covered entity, means—

(A) having the authority or ability to determine how the covered entity is utilized; or

(B) having some decisionmaking power for the use of the covered entity.

(4) COVERED ENTITY.—The term ''covered entity'' means—

(A) a person, corporation, company, business association, partnership, society, trust, or any other nongovernmental entity, organization, or group; or

(B) any governmental entity or instrumentality of a government.

(5) EXECUTIVE AGENCY.—The term ''Executive agency'' has the meaning given the term in section 105 of title 5, United States Code.

(6) FEDERAL AGENCY.—The term ''Federal agency'' means—

(A) an Executive agency; and

(B) any establishment in the legislative or judicial branch of the Federal Government.

(7) FEDERAL LESSEE.—

(A) IN GENERAL.—The term ''Federal lessee'' means—

(i) the Administrator;

(ii) the Architect of the Capitol; and

(iii) the head of any other Federal agency that has independent statutory leasing authority.

(B) EXCLUSIONS.—The term ''Federal lessee'' does not include—

(i) the head of an element of the intelligence community; or

(ii) the Secretary of Defense.

(8) FEDERAL TENANT.—

(A) IN GENERAL.—The term ''Federal tenant'' means a Federal agency that is occupying or will occupy a high-security leased space for which a lease agreement has been secured on behalf of the Federal agency.

(B) EXCLUSION.—The term ''Federal tenant'' does not include an element of the intelligence community.

(9) FOREIGN ENTITY.—The term ''foreign entity'' means—

(A) a corporation, company, business association, partnership, society, trust, or any other nongovernmental entity, organization,

or group that is headquartered in or organized under the laws of—

(i) a country that is not the United States; or

(ii) a State, unit of local government, or Indian Tribe that is not located within or a territory of the United States; or

(B) a government or governmental instrumentality that is not—

(i) the United States Government; or

(ii) a State, unit of local government, or Indian Tribe that is located within or a territory of the United States.

(10) FOREIGN PERSON.—The term ''foreign person'' means an individual who is not a United States person.

(11) HIGH-SECURITY LEASED ADJACENT SPACE.—The term ''high-security leased adjacent space'' means a building or office space that shares a boundary with or surrounds a high-security leased space.

(12) HIGH-SECURITY LEASED SPACE.—The term ''high-security leased space'' means a space leased by a Federal lessee that—

(A) will be occupied by Federal employees for nonmilitary activities; and

(B) has a facility security level of III, IV, or V, as determined by the Federal tenant in consultation with the Interagency Security Committee, the Secretary of Homeland Security, and the Administrator.

(13) HIGHEST-LEVEL OWNER.—The term ''highest-level owner'' means an entity that owns or controls—

(A) an immediate owner of the offeror of a lease for a high-security leased adjacent space; or

(B) 1 or more entities that control an immediate owner of the offeror of a lease described in subparagraph (A).

(14) IMMEDIATE OWNER.—The term ''immediate owner'' means an entity, other than the offeror of a lease for a high-security leased adjacent space, that has direct control of that offeror, including—

(A) ownership or interlocking management;

(B) identity of interests among family members;

(C) shared facilities and equipment; and

(D) the common use of employees.

(15) 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).

(16) SUBSTANTIAL ECONOMIC BENEFITS.—The term ''substantial economic benefits'', with respect to a natural person described in paragraph (2)(A)(ii), means having an entitlement to the funds or assets of a covered entity that, as a practical matter, enables the person, directly or indirectly, to control, manage, or direct the covered entity.

(17) UNITED STATES PERSON.—The term ''United States person'' means an individual who—

(A) is a citizen of the United States; or

(B) is an alien lawfully admitted for permanent residence in the United States.

(b) GOVERNMENT-WIDE STUDY.—

(1) COORDINATION STUDY.—The Administrator, in coordination with the Director of the Federal Protective Service, the Secretary of Homeland Security, the Director of the Office of Management and Budget, and any other relevant entities, as determined by the Administrator, shall carry out a Government-wide study examining options to assist agencies (as defined in section 551 of title 5, United States Code) to produce a security assessment process for high-security leased adjacent space before entering into a lease or novation agreement with a covered entity for the purposes of accommodating a Federal tenant located in a high-security leased space.

(2) CONTENTS.—The study required under paragraph (1)—

(A) shall evaluate how to produce a security assessment process that includes a process for assessing the threat level of each occupancy of a high-security leased adjacent space, including through—

(i) site-visits;

(ii) interviews; and

(iii) any other relevant activities determined necessary by the Director of the Federal Protective Service; and

(B) may include a process for collecting and using information on each immediate owner, highest-level owner, or beneficial owner of a covered entity that seeks to enter into a lease with a Federal lessee for a high-security leased adjacent space, including—

(i) name;

(ii) current residential or business street address; and

(iii) an identifying number or document that verifies identity as a United States person, a foreign person, or a foreign entity.

(3) WORKING GROUP.—

(A) IN GENERAL.—Not later than 90 days after the date of enactment of this Act, the Administrator, in coordination with the Director of Federal Protective Service, the Secretary of Homeland Security, the Director of the Office of Management and Budget, and any other relevant entities, as determined by the Administrator, shall establish a working group to assist in the carrying out of the study required under paragraph (1).

(B) NO COMPENSATION.—A member of the working group established under subparagraph (A) shall receive no compensation as a result of serving on the working group.

(C) SUNSET.—The working group established under subparagraph (A) shall terminate on the date on which the report required under paragraph (6) is submitted.

(4) PROTECTION OF INFORMATION.—The Administrator shall ensure that any information collected pursuant to the study required under paragraph (1) shall not be made available to the public.

(5) LIMITATION.—Nothing in this subsection requires an entity located in the United States to provide information requested pursuant to the study required under paragraph (1).

(6) REPORT.—Not later than 2 years after the date of enactment of this Act, the Administrator, in coordination with the Director of Federal Protective Service, the Secretary of Homeland Security, the Director of the Office of Management and Budget, and any other relevant entities, as determined by the Administrator, shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Transportation and Infrastructure of the House of Representatives a report describing—

(A) the results of the study required under paragraph (1); and

(B) how all applicable privacy laws and rights relating to the First and Fourth Amendments to the Constitution of the United States would be upheld and followed in—

(i) the security assessment process described in subparagraph (A) of paragraph (2); and

(ii) the information collection process described in subparagraph (B) of that paragraph.

(7) LIMITATION.—Nothing in this subsection authorizes a Federal entity to mandate information gathering unless specifically authorized by law.

(8) PROHIBITION.—No information collected pursuant the security assessment process described in paragraph (2)(A) may be used for law enforcement purposes.

(9) NO ADDITIONAL FUNDING.—No additional funds are authorized to be appropriated to carry out this subsection.

Subtitle B—Intergovernmental Critical Minerals Task Force

SEC. 6411. SHORT TITLE.

This subtitle may be cited as the ''Intergovernmental Critical Minerals Task Force Act''.

SEC. 6412. DEFINITIONS.

In this subtitle:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

(A) the Committees on Homeland Security and Governmental Affairs, Energy and Natural Resources, Armed Services, Environment and Public Works, Commerce, Science, and Transportation, and Foreign Relations of the Senate; and

(B) the Committees on Oversight and Accountability, Natural Resources, Armed Services, and Foreign Affairs of the House of Representatives.

(2) COVERED COUNTRY.—The term ''covered country'' means—

(A) a covered nation (as defined in section 4872(d) of title 10, United States Code); and

(B) any other country determined by the task force to be a geostrategic competitor or adversary of the United States with respect to critical minerals.

(3) CRITICAL MINERAL.—The term ''critical mineral'' has the meaning given the term in section 7002(a) of the Energy Act of 2020 (30 U.S.C. 1606(a)).

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

(5) TASK FORCE.—The term ''task force'' means the task force established under section 6414(b).

SEC. 6413. FINDINGS.

Congress finds that—

(1) current supply chains of critical minerals pose a great risk to the homeland and national security of the United States;

(2) critical minerals contribute to transportation, technology, renewable energy, military equipment and machinery, and other relevant entities crucial for the homeland and national security of the United States;

(3) in 2022, the United States was 100 percent import reliant for 12 out of 50 critical minerals and more than 50 percent import reliant for an additional 31 critical mineral commodities classified as ''critical'' by the United States Geological Survey, and the People's Republic of China was the top producing nation for 30 of those 50 critical minerals;

(4) companies based in the People's Republic of China that extract rare earth minerals around the world have received hundreds of charges of human rights violations; and

(5) on March 26, 2014, the World Trade Organization ruled that the export restraints by the People's Republic of China on rare earth metals violated obligations under the protocol of accession to the World Trade Organization, which harmed manufacturers and workers in the United States.

SEC. 6414. INTERGOVERNMENTAL CRITICAL MINERALS TASK FORCE.

(a) PURPOSES.—The purposes of the task force are—

(1) to assess the reliance of the United States on the People's Republic of China, and other covered countries, for critical minerals, and the resulting homeland and national security risks associated with that reliance, at each level of the Federal, State, local, Tribal, and territorial governments;

(2) to make recommendations to onshore and improve the domestic supply chain for critical minerals; and

(3) to reduce the reliance of the United States, and partners and allies of the United States, on critical mineral supply chains involving covered countries.

(b) ESTABLISHMENT.—Not later than 90 days after the date of enactment of this Act, the Director shall establish a task force to facilitate cooperation, coordination, and mutual accountability among each level of the Federal Government and State, local, Tribal, and territorial governments on a holistic response to the dependence on covered countries for critical minerals across the United States.

(c) COMPOSITION; MEETINGS.—

(1) APPOINTMENT.—The Director, in consultation with key intergovernmental, private, and public sector stakeholders, shall appoint to the task force representatives with expertise in critical mineral supply chains from Federal agencies, State, local, Tribal, and territorial governments, including not less than 1 representative from each of—

(A) the Bureau of Indian Affairs;
(B) the Bureau of Land Management;
(C) the Department of Agriculture;
(D) the Department of Commerce;
(E) the Department of Defense;
(F) the Department of Energy;
(G) the Department of Homeland Security;
(H) the Department of Housing and Urban Development;
(I) the Department of the Interior;
(J) the Department of Labor;
(K) the Department of State;
(L) the Department of Transportation;
(M) the Environmental Protection Agency;
(N) the General Services Administration;
(O) the National Science Foundation;
(P) the United States International Development Finance Corporation;
(Q) the United States Geological Survey; and
(R) any other relevant Federal entity, as determined by the Director.

(2) CONSULTATION.—The task force shall consult individuals with expertise in critical mineral supply chains, individuals from States whose communities, businesses, and industries are involved in aspects of the critical mineral supply chain, including mining and processing operations, and individuals from a diverse and balanced cross-section of—

(A) intergovernmental consultees, including—
(i) State governments;
(ii) local governments;
(iii) Tribal governments; and
(iv) territorial governments; and
(B) other stakeholders, including—
(i) academic research institutions;
(ii) corporations;
(iii) nonprofit organizations;
(iv) private sector stakeholders;
(v) trade associations;
(vi) mining industry stakeholders; and
(vii) labor representatives.

(3) CHAIR.—The Director may serve as chair of the task force, or designate a representative of the task force to serve as chair.

(4) MEETINGS.—

(A) INITIAL MEETING.—Not later than 90 days after the date on which all representatives of the task force have been appointed, the task force shall hold the first meeting of the task force.

(B) FREQUENCY.—The task force shall meet not less than once every 90 days.

(d) DUTIES.—

(1) IN GENERAL.—The duties of the task force shall include—

(A) facilitating cooperation, coordination, and mutual accountability for the Federal Government and State, local, Tribal, and territorial governments to enhance data sharing and transparency in the supply chains for critical minerals in support of the purposes described in subsection (a);

(B) providing recommendations with respect to—

(i) research and development into emerging technologies used to expand existing critical mineral supply chains in the United States and to establish secure and reliable critical mineral supply chains to the United States;

(ii) increasing capacities for mining, processing, refinement, reuse, and recycling of critical minerals in the United States to facilitate the environmentally responsible production of domestic resources to meet national critical mineral needs, in consultation with Tribal and local communities;

(iii) identifying how statutes, regulations, and policies related to the critical mineral supply chain could be modified to accelerate environmentally responsible domestic production of critical minerals, in consultation with Tribal and local communities;

(iv) strengthening the domestic workforce to support growing critical mineral supply chains with good-paying, safe jobs in the United States;

(v) identifying alternative domestic sources to critical minerals that the United States currently relies on the People's Republic of China or other covered countries for mining, processing, refining, and recycling, including the availability, cost, and quality of those domestic alternatives;

(vi) identifying critical minerals and critical mineral supply chains that the United States can onshore, at a competitive availability, cost, and quality, for those minerals and supply chains that the United States relies on the People's Republic of China or other covered countries to provide; and

(vii) opportunities for the Federal Government and State, local, Tribal, and territorial governments to mitigate risks to the homeland and national security of the United States with respect to supply chains for critical minerals that the United States currently relies on the People's Republic of China or other covered countries for mining, processing, refining, and recycling;

(C) prioritizing the recommendations in subparagraph (B), taking into consideration economic costs and focusing on the critical mineral supply chains with vulnerabilities posing the most significant risks to the homeland and national security of the United States;

(D) establishing specific strategies, to be carried out in coordination with the Secretary of State, to strengthen international partnerships in furtherance of critical minerals supply chain security with international allies and partners, including—

(i) countries with which the United States has a free trade agreement;

(ii) countries participating in the Indo-Pacific Economic Framework for Prosperity;

(iii) countries participating in the Quadrilateral Security Dialogue;

(iv) countries that are signatories to the Abraham Accords;

(v) countries designated as eligible sub-Saharan Africa countries under section 104 of the Africa Growth and Opportunity Act (19 U.S.C. 3701 et seq.); and

(vi) other countries or multilateral partnerships the Task Force determines to be appropriate; and

(E) other duties, as determined by the Director.

(2) REPORT.—The Director shall—

(A) not later than 2 years after the date of enactment of this Act, submit to the appropriate committees of Congress a report, which shall be submitted in unclassified form, but may include a classified annex, that describes any findings, guidelines, and recommendations created in performing the duties under paragraph (1);

(B) not later than 120 days after the date on which the Director submits the report under subparagraph (A), publish that report in the Federal Register and on the website of the Office of Management and Budget, except that the Director shall redact information from the report that the Director determines could pose a risk to the homeland and national security of the United States by being publicly available; and

(C) brief the appropriate committees of Congress twice per year.

(e) SUNSET.—The task force shall terminate on the date that is 90 days after the date on which the task force completes the requirements under subsection (d)(2).

(f) GAO STUDY.—

(1) IN GENERAL.—The Comptroller General of the United States shall conduct a study examining the Federal and State regulatory landscape related to improving domestic supply chains for critical minerals in the United States.

(2) REPORT.—Not later than 18 months after the date of enactment of this Act, the Comptroller General of the United States shall submit to the appropriate committees of Congress a report that describes the results of the study under paragraph (1).

DIVISION G—COMMITTEE ON FOREIGN RELATIONS

TITLE LXX—AUKUS MATTERS

SEC. 7001. DEFINITIONS.

In this title:

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

(A) the Committee on Foreign Relations and the Committee on Armed Services of the Senate; and

(B) the Committee on Foreign Affairs and the Committee on Armed Services of the House of Representatives.

(2) AUKUS PARTNERSHIP.—

(A) IN GENERAL.—The term ''AUKUS partnership'' means the enhanced trilateral security partnership between Australia, the United Kingdom, and the United States announced in September 2021.

(B) PILLARS.—The AUKUS partnership includes the following two pillars:

(i) Pillar One is focused on developing a pathway for Australia to acquire conventionally armed, nuclear-powered submarines.

(ii) Pillar Two is focused on enhancing trilateral collaboration on advanced defense capabilities, including hypersonic and counter hypersonic capabilities, quantum technologies, undersea technologies, and artificial intelligence.

(3) DEPARTMENT.—The term ''Department'' means the Department of State.

(4) INTERNATIONAL TRAFFIC IN ARMS REGULATIONS.—The term ''International Traffic in Arms Regulations'' means subchapter M of chapter I of title 22, Code of Federal Regulations (or successor regulations).

(5) SECRETARY.—The term ''Secretary'' means the Secretary of State.

Subtitle A—Outlining the AUKUS Partnership

SEC. 7011. STATEMENT OF POLICY ON THE AUKUS PARTNERSHIP.

(a) STATEMENT OF POLICY.—It is the policy of the United States that—

(1) the AUKUS partnership is integral to United States national security, increasing United States and allied capability in the undersea domain of the Indo-Pacific, and developing cutting edge military capabilities;

(2) the transfer of conventionally armed, nuclear-powered submarines to Australia will position the United States and its allies to maintain peace and security in the Indo-Pacific;

(3) the transfer of conventionally armed, nuclear-powered submarines to Australia

will be safely implemented with the highest nonproliferation standards in alignment with—

(A) safeguards established by the International Atomic Energy Agency; and

(B) the Additional Protocol to the Agreement between Australia and the International Atomic Energy Agency for the application of safeguards in connection with the Treaty on the Non-Proliferation of Nuclear Weapons, signed at Vienna September 23, 1997;

(4) the United States will enter into a mutual defense agreement with Australia, modeled on the 1958 bilateral mutual defense agreement with the United Kingdom, for the sole purpose of facilitating the transfer of naval nuclear propulsion technology to Australia;

(5) working with the United Kingdom and Australia to develop and provide joint advanced military capabilities to promote security and stability in the Indo-Pacific will have tangible impacts on United States military effectiveness across the world;

(6) in order to better facilitate cooperation under Pillar 2 of the AUKUS partnership, it is imperative that every effort be made to streamline United States export controls consistent with necessary and reciprocal security safeguards on United States technology at least comparable to those of the United States;

(7) the trade authorization mechanism for the AUKUS partnership administered by the Department is a critical first step in reimagining the United States export control system to carry out the AUKUS partnership and expedite technology sharing and defense trade among the United States, Australia, and the United Kingdom; and

(8) the vast majority of United States defense trade with Australia is conducted through the Foreign Military Sales (FMS) process, the preponderance of defense trade with the United Kingdom is conducted through Direct Commercial Sales (DCS), and efforts to streamline United States export controls should focus on both Foreign Military Sales and Direct Commercial Sales.

SEC. 7012. SENIOR ADVISOR FOR THE AUKUS PARTNERSHIP AT THE DEPARTMENT OF STATE.

(a) IN GENERAL.—There shall be a Senior Advisor for the AUKUS partnership at the Department, who—

(1) shall report directly to the Secretary; and

(2) may not hold another position in the Department concurrently while holding the position of Senior Advisor for the AUKUS partnership.

(b) DUTIES.—The Senior Advisor shall—

(1) be responsible for coordinating efforts related to the AUKUS partnership across the Department, including the bureaus engaged in nonproliferation, defense trade, security assistance, and diplomatic relations in the Indo-Pacific;

(2) serve as the lead within the Department for implementation of the AUKUS partnership in interagency processes, consulting with counterparts in the Department of Defense, the Department of Commerce, the Department of Energy, the Office of Naval Reactors, and any other relevant agencies;

(3) lead diplomatic efforts related to the AUKUS partnership with other governments to explain how the partnership will enhance security and stability in the Indo-Pacific; and

(4) consult regularly with the appropriate congressional committees, and keep such committees fully and currently informed, on issues related to the AUKUS partnership, including in relation to the AUKUS Pillar 1 objective of supporting Australia's acquisition of conventionally armed, nuclear-powered submarines and the Pillar 2 objective of jointly developing advanced military capabilities to support security and stability in the Indo-Pacific, as affirmed by the President of the United States, the Prime Minister of the United Kingdom, and the Prime Minister of Australia on April 5, 2022.

(c) PERSONNEL TO SUPPORT THE SENIOR ADVISOR.—The Secretary shall ensure that the Senior Advisor is adequately staffed, including through encouraging details, or assignment of employees of the Department, with expertise related to the implementation of the AUKUS partnership, including staff with expertise in—

(1) nuclear policy, including nonproliferation;

(2) defense trade and security cooperation, including security assistance; and

(3) relations with respect to political-military issues in the Indo-Pacific and Europe.

(d) NOTIFICATION.—Not later than 180 days after the date of the enactment of this Act, and not later than 90 days after a Senior Advisor assumes such position, the Secretary shall notify the appropriate congressional committees of the number of full-time equivalent positions, relevant expertise, and duties of any employees of the Department or detailees supporting the Senior Advisor.

(e) SUNSET.—

(1) IN GENERAL.—The position of the Senior Advisor for the AUKUS partnership shall terminate on the date that is 8 years after the date of the enactment of this Act.

(2) RENEWAL.—The Secretary may renew the position of the Senior Advisor for the AUKUS partnership for 1 additional period of 4 years, following notification to the appropriate congressional committees of the renewal.

Subtitle B—Authorization for Submarine Transfers, Support, and Infrastructure Improvement Activities

SEC. 7021. AUSTRALIA, UNITED KINGDOM, AND UNITED STATES SUBMARINE SECURITY ACTIVITIES.

(a) AUTHORIZATION TO TRANSFER SUBMARINES.—

(1) IN GENERAL.—Subject to paragraphs (3), (4), and (11), the President may, under section 21 of the Arms Export Control Act (22 U.S.C. 2761)—

(A) transfer not more than two Virginia class submarines from the inventory of the United States Navy to the Government of Australia on a sale basis; and

(B) transfer not more than one additional Virginia class submarine to the Government of Australia on a sale basis.

(2) REQUIREMENTS NOT APPLICABLE.—A sale carried out under paragraph (1)(B) shall not be subject to the requirements of—

(A) section 36 of the Arms Export Control Act (22 U.S.C. 2776); or

(B) section 8677 of title 10, United States Code.

(3) CERTIFICATION; BRIEFING.—

(A) PRESIDENTIAL CERTIFICATION.—The President may exercise the authority provided by paragraph (1) not earlier than 60 days after the date on which the President certifies to the appropriate congressional committees that any submarine transferred under such authority shall be used to support the joint security interests and military operations of the United States and Australia.

(B) WAIVER OF CHIEF OF NAVAL OPERATIONS CERTIFICATION.—The requirement for the Chief of Naval Operations to make a certification under section 8678 of title 10, United States Code, shall not apply to a transfer under paragraph (1).

(C) BRIEFING.—Not later than 90 days before the sale of any submarine under paragraph (1), the Secretary of the Navy shall provide to the appropriate congressional committees a briefing on—

(i) the impacts of such sale to the readiness of the submarine fleet of the United States, including with respect to maintenance timelines, deployment-to-dwell ratios, training, exercise participation, and the ability to meet combatant commander requirements;

(ii) the impacts of such sale to the submarine industrial base of the United States, including with respect to projected maintenance requirements, acquisition timelines for spare and replacement parts, and future procurement of Virginia class submarines for the submarine fleet of the United States; and

(iii) other relevant topics as determined by the Secretary of the Navy.

(4) REQUIRED MUTUAL DEFENSE AGREEMENT.—Before any transfer occurs under subsection (a), the United States and Australia shall have a mutual defense agreement in place, which shall—

(A) provide a clear legal framework for the sole purpose of Australia's acquisition of conventionally armed, nuclear-powered submarines; and

(B) meet the highest nonproliferation standards for the exchange of nuclear materials, technology, equipment, and information between the United States and Australia.

(5) SUBSEQUENT SALES.—A sale of a Virginia class submarine that occurs after the sales described in paragraph (1) may occur only if such sale is explicitly authorized in legislation enacted after the date of the enactment of this Act.

(6) COSTS OF TRANSFER.—Any expense incurred by the United States in connection with a transfer under paragraph (1) shall be charged to the Government of Australia.

(7) CREDITING OF RECEIPTS.—Notwithstanding any provision of law pertaining to the crediting of amounts received from a sale under section 21 of the Arms Export Control Act (22 U.S.C. 2761), any funds received by the United States pursuant to a transfer under paragraph (1) shall—

(A) be credited, at the discretion of the President, to—

(i) the fund or account used in incurring the original obligation for the acquisition of submarines transferred under paragraph (1);

(ii) an appropriate fund or account available for the purposes for which the expenditures for the original acquisition of submarines transferred under paragraph (1) were made; or

(iii) any other fund or account available for the purpose specified in paragraph (8)(B); and

(B) remain available for obligation until expended.

(8) USE OF FUNDS.—Subject to paragraphs (9) and (10), the President may use funds received pursuant to a transfer under paragraph (1)—

(A) for the acquisition of submarines to replace the submarines transferred to the Government of Australia; or

(B) for improvements to the submarine industrial base of the United States.

(9) PLAN FOR USE OF FUNDS.—Before any use of any funds received pursuant to a transfer under paragraph (1), the President shall submit to the appropriate congressional committees, the Committee on Appropriations of the Senate, and the Committee on Appropriations of the House of Representatives a plan detailing how such funds will be used, including specific amounts and purposes.

(10) NOTIFICATION AND REPORT.—

(A) NOTIFICATION.—Not later than 30 days after the date of any transfer under paragraph (1), and upon any transfer or depositing of funds received pursuant to such a transfer, the President shall notify the appropriate congressional committees, the

Committee on Appropriations of the Senate, and the Committee on Appropriations of the House of Representatives of—

(i) the amount of funds received pursuant to the transfer; and

(ii) the specific account or fund into which the funds described in clause (i) are deposited.

(B) ANNUAL REPORT.—Not later than November 30 of each year until 1 year after the date on which all funds received pursuant to transfers under paragraph (1) have been fully expended, the President shall submit to the committees described in subparagraph (A) a report that includes an accounting of how funds received pursuant to transfers under paragraph (1) were used in the fiscal year preceding the fiscal year in which the report is submitted.

(11) APPLICABILITY OF EXISTING LAW TO TRANSFER OF SPECIAL NUCLEAR MATERIAL AND UTILIZATION FACILITIES FOR MILITARY APPLICATIONS.—

(A) IN GENERAL.—With respect to any special nuclear material for use in utilization facilities or any portion of a submarine transferred under paragraph (1) constituting utilization facilities for military applications under section 91 of the Atomic Energy Act of 1954 (42 U.S.C. 2121), transfer of such material or such facilities shall occur only in accordance with such section 91.

(B) USE OF FUNDS.—The President may use proceeds from a transfer described in subparagraph (A) for the acquisition of submarine naval nuclear propulsion plants and nuclear fuel to replace propulsion plants and fuel transferred to the Government of Australia.

(b) REPAIR AND REFURBISHMENT OF AUKUS SUBMARINES.—Section 8680 of title 10, United States Code, is amended—

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

(2) by inserting after subsection (b) the following new subsection (c):

''(c) REPAIR AND REFURBISHMENT OF CERTAIN SUBMARINES.—

''(1) SHIPYARD.—Notwithstanding any other provision of this section, the President shall—

''(A) determine the appropriate shipyard in the United States, Australia, or the United Kingdom to perform any repair or refurbishment of a United States submarine involved in submarine security activities between the United States, Australia, and the United Kingdom; and

''(B) in making a determination under subparagraph (A) with respect whether a shipyard is appropriate, consider the significance of the shipyard to strategically important areas of operations.

''(2) PERSONNEL.—Repair or refurbishment described in paragraph (1)(A) may be carried out by personnel of the United States, the United Kingdom, or Australia in accordance with the international arrangements governing the submarine security activities described in such paragraph.''.

SEC. 7022. ACCEPTANCE OF CONTRIBUTIONS FOR AUSTRALIA, UNITED KINGDOM, AND UNITED STATES SUBMARINE SECURITY ACTIVITIES; AUKUS SUBMARINE SECURITY ACTIVITIES ACCOUNT.

(a) ACCEPTANCE AUTHORITY.—The President may accept from the Government of Australia contributions of money made by the Government of Australia for use by the Department of Defense in support of non-nuclear related aspects of submarine security activities between Australia, the United Kingdom, and the United States (AUKUS).

(b) ESTABLISHMENT OF AUKUS SUBMARINE SECURITY ACTIVITIES ACCOUNT.—

(1) IN GENERAL.—There is established in the Treasury of the United States a special account to be known as the ''AUKUS Submarine Security Activities Account''.

(2) CREDITING OF CONTRIBUTIONS OF MONEY.—Contributions of money accepted by the President under subsection (a) shall be credited to the AUKUS Submarine Security Activities Account.

(3) AVAILABILITY.—Amounts credited to the AUKUS Submarine Security Activities Account shall remain available until expended.

(c) USE OF AUKUS SUBMARINE SECURITY ACTIVITIES ACCOUNT.—

(1) IN GENERAL.—Subject to paragraph (2), the President may use funds in the AUKUS Submarine Security Activities Account—

(A) for any purpose authorized by law that the President determines would support submarine security activities between Australia, the United Kingdom, and the United States; or

(B) to carry out a military construction project related to the AUKUS partnership that is not otherwise authorized by law.

(2) PLAN FOR USE OF FUNDS.—Before any use of any funds in the AUKUS Submarine Security Activities Account, the President shall submit to the appropriate congressional committees, the Committee on Appropriations of the Senate, and the Committee on Appropriations of the House of Representatives a plan detailing—

(A) the amount of funds in the AUKUS Submarine Security Activities Account; and

(B) how such funds will be used, including specific amounts and purposes.

(d) TRANSFERS OF FUNDS.—

(1) IN GENERAL.—In carrying out subsection (c) and subject to paragraphs (2) and (5), the President may transfer funds available in the AUKUS Submarine Security Activities Account to an account or fund available to the Department of Defense or any other appropriate agency.

(2) DEPARTMENT OF ENERGY.—In carrying out subsection (c), and in accordance with the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.), the President may transfer funds available in the AUKUS Submarine Security Activities Account to an account or fund available to the Department of Energy to carry out activities related to submarine security activities between Australia, the United Kingdom, and the United States.

(3) AVAILABILITY FOR OBLIGATION.—Funds transferred under this subsection shall be available for obligation for the same time period and for the same purpose as the account or fund to which transferred.

(4) TRANSFER BACK TO ACCOUNT.—Upon a determination by the President that all or part of the funds transferred from the AUKUS Submarine Security Activities Account are not necessary for the purposes for which such funds were transferred, and subject to paragraph (5), all or such part of such funds shall be transferred back to the AUKUS Submarine Security Activities Account.

(5) NOTIFICATION AND REPORT.—

(A) NOTIFICATION.—The President shall notify the appropriate congressional committees, the Committee on Appropriations of the Senate, and the Committee on Appropriations of the House of Representatives of—

(i) before the transfer of any funds under this subsection—

(I) the amount of funds to be transferred; and

(II) the planned or anticipated purpose of such funds; and

(ii) before the obligation of any funds transferred under this subsection—

(I) the amount of funds to be obligated; and

(II) the purpose of the obligation.

(B) ANNUAL REPORT.—Not later than November 30 of each year until 1 year after the date on which all funds transferred under this subsection have been fully expended, the President shall submit to the committees described in subparagraph (A) a report that includes a detailed accounting of—

(i) the amount of funds transferred under this subsection during the fiscal year preceding the fiscal year in which the report is submitted; and

(ii) the purposes for which such funds were used.

(e) INVESTMENT OF MONEY.—

(1) AUTHORIZED INVESTMENTS.—The President may invest money in the AUKUS Submarine Security Activities Account in securities of the United States or in securities guaranteed as to principal and interest by the United States.

(2) INTEREST AND OTHER INCOME.—Any interest or other income that accrues from investment in securities referred to in paragraph (1) shall be deposited to the credit of the AUKUS Submarine Security Activities Account.

(f) RELATIONSHIP TO OTHER LAWS.—The authority to accept or transfer funds under this section is in addition to any other authority to accept or transfer funds.

SEC. 7023. AUSTRALIA, UNITED KINGDOM, AND UNITED STATES SUBMARINE SECURITY TRAINING.

(a) IN GENERAL.—The President may transfer or export directly to private individuals in Australia defense services that may be transferred to the Government of Australia under the Arms Export Control Act (22 U.S.C. 2751 et seq.) to support the development of the submarine industrial base of Australia necessary for submarine security activities between Australia, the United Kingdom, and the United States, including if such individuals are not officers, employees, or agents of the Government of Australia.

(b) SECURITY CONTROLS.—

(1) IN GENERAL.—Any defense service transferred or exported under subsection (a) shall be subject to appropriate security controls to ensure that any sensitive information conveyed by such transfer or export is protected from disclosure to persons unauthorized by the United States to receive such information.

(2) CERTIFICATION.—Not later than 30 days before the first transfer or export of a defense service under subsection (a), and annually thereafter, the President shall certify to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives that the controls described in paragraph (1) will protect the information described in such paragraph for the defense services so transferred or exported.

(c) APPLICATION OF REQUIREMENTS FOR RETRANSFER AND REEXPORT.—Any person who receives any defense service transferred or exported under subsection (a) may retransfer or reexport such service to other persons only in accordance with the requirements of the Arms Export Control Act (22 U.S.C. 2751 et seq.).

Subtitle C—Streamlining and Protecting Transfers of United States Military Technology From Compromise

SEC. 7031. PRIORITY FOR AUSTRALIA AND THE UNITED KINGDOM IN FOREIGN MILITARY SALES AND DIRECT COMMERCIAL SALES.

(a) IN GENERAL.—The President shall institute policies and procedures for letters of request from Australia and the United Kingdom to transfer defense articles and services under section 21 of the Arms Export Control Act (22 U.S.C. 2761) related to the AUKUS partnership to receive expedited consideration and processing relative to all other letters of request other than from Taiwan and Ukraine.

(b) TECHNOLOGY TRANSFER POLICY FOR AUSTRALIA, CANADA, AND THE UNITED KINGDOM.—

(1) IN GENERAL.—The Secretary, in consultation with the Secretary of Defense, shall create an anticipatory release policy for the transfer of technologies described in paragraph (2) to Australia, the United Kingdom, and Canada through Foreign Military Sales and Direct Commercial Sales that are not covered by an exemption under the International Traffic in Arms Regulations.

(2) CAPABILITIES DESCRIBED.—The capabilities described in this paragraph are—

(A) Pillar One-related technologies associated with submarine and associated combat systems; and

(B) Pillar Two-related technologies, including hypersonic missiles, cyber capabilities, artificial intelligence, quantum technologies, undersea capabilities, and other advanced technologies.

(3) EXPEDITED DECISION-MAKING.—Review of a transfer under the policy established under paragraph (1) shall be subject to an expedited decision-making process.

(c) INTERAGENCY POLICY AND GUIDANCE.—The Secretary and the Secretary of Defense shall jointly review and update interagency policies and implementation guidance related to requests for Foreign Military Sales and Direct Commercial Sales, including by incorporating the anticipatory release provisions of this section.

SEC. 7032. IDENTIFICATION AND PRE-CLEARANCE OF PLATFORMS, TECHNOLOGIES, AND EQUIPMENT FOR SALE TO AUSTRALIA AND THE UNITED KINGDOM THROUGH FOREIGN MILITARY SALES AND DIRECT COMMERCIAL SALES.

Not later than 90 days after the date of the enactment of this Act, and on a biennial basis thereafter for 8 years, the President shall submit to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives a report that includes a list of advanced military platforms, technologies, and equipment that are pre-cleared and prioritized for sale and release to Australia, the United Kingdom and Canada through the Foreign Military Sales and Direct Commercial Sales programs without regard to whether a letter of request or license to purchase such platforms, technologies, or equipment has been received from any of such country. Each list may include items that are not related to the AUKUS partnership but may not include items that are not covered by an exemption under the International Traffic in Arms Regulations.

SEC. 7033. EXPORT CONTROL EXEMPTIONS AND STANDARDS.

(a) IN GENERAL.—Section 38 of the Arms Export Control Act of 1976 (22 U.S.C. 2778) is amended by adding at the end the following new subsection:

''(l) AUKUS DEFENSE TRADE COOPERATION.—

''(1) EXEMPTION FROM LICENSING AND APPROVAL REQUIREMENTS.—Subject to paragraph (2) and notwithstanding any other provision of this section, the Secretary of State may exempt from the licensing or other approval requirements of this section exports and transfers (including reexports, retransfers, temporary imports, and brokering activities) of defense articles and defense services between or among the United States, the United Kingdom, and Australia that—

''(A) are not excluded by those countries;

''(B) are not referred to in subsection(j)(1)(C)(ii); and

''(C) involve only persons or entities that are approved by—

''(i) the Secretary of State; and

''(ii) the Ministry of Defense, the Ministry of Foreign Affairs, or other similar authority within those countries.

''(2) LIMITATION.—The authority provided in subparagraph (1) shall not apply to any activity, including exports, transfers, reexports, retransfers, temporary imports, or brokering, of United States defense articles and defense services involving any country or a person or entity of any country other than the United States, the United Kingdom, and Australia.''.

(b) REQUIRED STANDARDS OF EXPORT CONTROLS.—The Secretary may only exercise the authority under subsection (l)(1) of section 38 of the Arms Export Control Act of 1976, as added by subsection (a) of this section, with respect to the United Kingdom or Australia 30 days after the Secretary submits to the appropriate congressional committees an unclassified certification and detailed unclassified assessment (which may include a classified annex) that the country concerned has implemented standards for a system of export controls that satisfies the elements of section 38(j)(2) of the Arms Export Control Act (22 U.S.C. 2778(j)(2)) for United States-origin defense articles and defense services, and for controlling the provision of military training, that are comparable to those standards administered by the United States in effect on the date of the enactment of this Act.

(c) CERTAIN REQUIREMENTS NOT APPLICABLE.—

(1) IN GENERAL.—Paragraphs (1), (2), and (3) of section 3(d) of the Arms Export Control Act (22 U.S.C. 2753(d)) shall not apply to any export or transfer that is the subject of an exemption under subsection (l)(1) of section 38 of the Arms Export Control Act of 1976, as added by subsection (a) of this section.

(2) QUARTERLY REPORTS.—The Secretary shall—

(A) require all exports and transfers that would be subject to the requirements of paragraphs (1), (2), and (3) of section 3(d) of the Arms Export Control Act (22 U.S.C. 2753(d)) but for the application of subsection (l)(1) of section 38 of the Arms Export Control Act of 1976, as added by subsection (a) of this section, to be reported to the Secretary; and

(B) submit such reports to the Committee on Foreign Relations of the Senate and Committee on Foreign Affairs of the House of Representatives on a quarterly basis.

(d) SUNSET.—Any exemption under subsection (l)(1) of section 38 of the Arms Export Control Act of 1976, as added by subsection (a) of this section, shall terminate on the date that is 15 years after the date of the enactment of this Act. The Secretary of State may renew such exemption for 5 years upon a certification to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives that such exemption is in the vital national interest of the United States with a detailed justification for such certification.

(e) REPORTS.—

(1) ANNUAL REPORT.—

(A) IN GENERAL.—Not later than one year after the date of the enactment of this Act, and annually thereafter until no exemptions under subsection (l)(1) of section 38 of the Arms Export Control Act of 1976, as added by subsection (a) of this section, remain in effect, the Secretary shall submit to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives a report on the operation of exemptions issued under such subsection (l)(1), including whether any changes to such exemptions are likely to be made in the coming year.

(B) INITIAL REPORT.—The first report submitted under subparagraph (A) shall also include an assessment of key recommendations the United States Government has provided to the Governments of Australia and the United Kingdom to revise laws, regulations, and policies of such countries that are required to implement the AUKUS partnership.

(2) REPORT ON EXPEDITED REVIEW OF EXPORT LICENSES FOR EXPORTS OF ADVANCED TECHNOLOGIES.—Not later than 180 days after the date of the enactment of this Act, the Secretary of State, in coordination with the Secretary of Defense, shall report on the practical application of a possible ''fast track'' decision-making process for applications, classified or unclassified, to export defense articles and defense services to Australia, the United Kingdom, and Canada.

SEC. 7034. EXPEDITED REVIEW OF EXPORT LICENSES FOR EXPORTS OF ADVANCED TECHNOLOGIES TO AUSTRALIA, THE UNITED KINGDOM, AND CANADA.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary, in coordination with the Secretary of Defense, shall initiate a rulemaking to establish an expedited decision-making process, classified or unclassified, for applications to export to Australia, the United Kingdom, and Canada commercial, advanced-technology defense articles and defense services that are not covered by an exemption under the International Traffic in Arms Regulations.

(b) ELIGIBILITY.—To qualify for the expedited decision-making process described in subsection (a), an application shall be for an export of defense articles or defense services that will take place wholly within or between the physical territory of Australia, Canada, or the United Kingdom and the United States and with governments or corporate entities from such countries.

(c) AVAILABILITY OF EXPEDITED PROCESS.—The expedited decision-making process described in subsection (a) shall be available for both classified and unclassified items, and the process must satisfy the following criteria to the extent practicable:

(1) Any licensing application to export defense articles and services that is related to a government to government AUKUS agreement must be approved, returned, or denied withing 30 days of submission.

(2) For all other licensing requests, any review shall be completed not later than 45 calendar days after the date of application.

SEC. 7035. UNITED STATES MUNITIONS LIST.

(a) EXEMPTION FOR THE GOVERNMENTS OF THE UNITED KINGDOM AND AUSTRALIA FROM CERTIFICATION AND CONGRESSIONAL NOTIFICATION REQUIREMENTS APPLICABLE TO CERTAIN TRANSFERS.—Section 38(f)(3) of the Arms Export Control Act (22 U.S.C. 2778(f)(3)) is amended by inserting '', the United Kingdom, or Australia'' after ''Canada''.

(b) UNITED STATES MUNITIONS LIST PERIODIC REVIEWS.—

(1) IN GENERAL.—The Secretary, acting through authority delegated by the President to carry out periodic reviews of items on the United States Munitions List under section 38(f) of the Arms Export Control Act (22 U.S.C. 2778(f)) and in coordination with the Secretary of Defense, the Secretary of Energy, the Secretary of Commerce, and the Director of the Office of Management and Budget, shall carry out such reviews not less frequently than every 3 years.

(2) SCOPE.—The periodic reviews described in paragraph (1) shall focus on matters including—

(A) interagency resources to address current threats faced by the United States;

(B) the evolving technological and economic landscape;

(C) the widespread availability of certain technologies and items on the United States Munitions List; and

(D) risks of misuse of United States-origin defense articles.

(3) CONSULTATION.—The Department of State may consult with the Defense Trade Advisory Group (DTAG) and other interested

parties in conducting the periodic review described in paragraph (1).

Subtitle D—Other AUKUS Matters

SEC. 7041. REPORTING RELATED TO THE AUKUS PARTNERSHIP.

(a) REPORT ON INSTRUMENTS.—

(1) IN GENERAL.—Not later than 30 days after the signature, conclusion, or other finalization of any non-binding instrument related to the AUKUS partnership, the President shall submit to the appropriate congressional committees the text of such instrument.

(2) NON-DUPLICATION OF EFFORTS; RULE OF CONSTRUCTION.—To the extent the text of a non-binding instrument is submitted to the appropriate congressional committees pursuant to subsection (a), such text does not need to be submitted to Congress pursuant to section 112b(a)(1)(A)(ii) of title 1, United States Code, as amended by section 5947 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Public Law 117–263; 136 Stat. 3476). Paragraph (1) shall not be construed to relieve the executive branch of any other requirement of section 112b of title 1, United States Code, as amended so amended, or any other provision of law.

(3) DEFINITIONS.—In this section:

(A) IN GENERAL.—The term ''text'', with respect to a non-binding instrument, includes—

(i) any annex, appendix, codicil, side agreement, side letter, or any document of similar purpose or function to the aforementioned, regardless of the title of the document, that is entered into contemporaneously and in conjunction with the non-binding instrument; and

(ii) any implementing agreement or arrangement, or any document of similar purpose or function to the aforementioned, regardless of the title of the document, that is entered into contemporaneously and in conjunction with the non-binding instrument.

(B) CONTEMPORANEOUSLY AND IN CONJUNCTION WITH.—As used in subparagraph (A), the term ''contemporaneously and in conjunction with''—

(i) shall be construed liberally; and

(ii) may not be interpreted to require any action to have occurred simultaneously or on the same day.

(b) REPORT ON AUKUS PARTNERSHIP.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, and biennially thereafter, the Secretary, in coordination with the Secretary of Defense and other appropriate heads of agencies, shall submit to the appropriate congressional committees a report on the AUKUS partnership.

(2) ELEMENTS.—Each report required under paragraph (1) shall include the following elements:

(A) STRATEGY.—

(i) An identification of the defensive military capability gaps and capacity shortfalls that the AUKUS partnership seeks to offset.

(ii) An explanation of the total cost to the United States associated with Pillar One of the AUKUS partnership.

(iii) A detailed explanation of how enhanced access to the industrial base of Australia is contributing to strengthening the United States strategic position in Asia.

(iv) A detailed explanation of the military and strategic benefit provided by the improved access provided by naval bases of Australia.

(v) A detailed assessment of how Australia's sovereign conventionally armed nuclear attack submarines contribute to United States defense and deterrence objectives in the Indo-Pacific region.

(B) IMPLEMENT THE AUKUS PARTNERSHIP.—

(i) Progress made on achieving the Optimal Pathway established for Australia's development of conventionally armed, nuclear-powered submarines, including the following elements:

(I) A description of progress made by Australia, the United Kingdom, and the United States to conclude an Article 14 arrangement with the International Atomic Energy Agency.

(II) A description of the status of efforts of Australia, the United Kingdom, and the United States to build the supporting infrastructure to base conventionally armed, nuclear-powered attack submarines.

(III) Updates on the efforts by Australia, the United Kingdom, and the United States to train a workforce that can build, sustain, and operate conventionally armed, nuclear-powered attack submarines.

(IV) A description of progress in establishing submarine support facilities capable of hosting rotational forces in western Australia by 2027.

(V) A description of progress made in improving United States submarine production capabilities that will enable the United States to meet—

(aa) its objectives of providing up to five Virginia Class submarines to Australia by the early to mid-2030's; and

(bb) United States submarine production requirements.

(ii) Progress made on Pillar Two of the AUKUS partnership, including the following elements:

(I) An assessment of the efforts of Australia, the United Kingdom, and the United States to enhance collaboration across the following eight trilateral lines of effort:

(aa) Underseas capabilities.

(bb) Quantum technologies.

(cc) Artificial intelligence and autonomy.

(dd) Advanced cyber capabilities.

(ee) Hypersonic and counter-hypersonic capabilities.

(ff) Electronic warfare.

(gg) Innovation.

(hh) Information sharing.

(II) An assessment of any new lines of effort established.

DIVISION H—COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

TITLE LXXX—SECURING SEMICONDUCTOR SUPPLY CHAINS ACT OF 2023

SEC. 8001. SHORT TITLE.

This title may be cited as the ''Securing Semiconductor Supply Chains Act of 2023''.

SEC. 8002. SELECTUSA DEFINED.

In this title, the term ''SelectUSA'' means the SelectUSA program of the Department of Commerce established by Executive Order 13577 (76 Fed. Reg. 35,715).

SEC. 8003. FINDINGS.

Congress makes the following findings:

(1) Semiconductors underpin the United States and global economies, including manufacturing sectors. Semiconductors are also essential to the national security of the United States.

(2) A shortage of semiconductors, brought about by the COVID–19 pandemic and other complex factors impacting the overall supply chain, has threatened the economic recovery of the United States and industries that employ millions of United States citizens.

(3) Addressing current challenges and building resilience against future risks requires ensuring a secure and stable supply chain for semiconductors that will support the economic and national security needs of the United States and its allies.

(4) The supply chain for semiconductors is complex and global. While the United States plays a leading role in certain segments of the semiconductor industry, securing the supply chain requires onshoring, reshoring, or diversifying vulnerable segments, such as for—

(A) fabrication;

(B) advanced packaging; and

(C) materials and equipment used to manufacture semiconductor products.

(5) The Federal Government can leverage foreign direct investment and private dollars to grow the domestic manufacturing and production capacity of the United States for vulnerable segments of the semiconductor supply chain.

(6) The SelectUSA program of the Department of Commerce, in coordination with other Federal agencies and State-level economic development organizations, is positioned to boost foreign direct investment in domestic manufacturing and to help secure the semiconductor supply chain of the United States.

SEC. 8004. COORDINATION WITH STATE-LEVEL ECONOMIC DEVELOPMENT ORGANIZATIONS.

Not later than 180 days after the date of the enactment of this Act, the Executive Director of SelectUSA shall solicit comments from State-level economic development organizations—

(1) to review—

(A) what efforts the Federal Government can take to support increased foreign direct investment in any segment of semiconductor-related production;

(B) what barriers to such investment may exist and how to amplify State efforts to attract such investment;

(C) public opportunities those organizations have identified to attract foreign direct investment to help increase investment described in subparagraph (A); and

(D) resource gaps or other challenges that prevent those organizations from increasing such investment; and

(2) to develop recommendations for—

(A) how SelectUSA can increase such investment independently or through partnership with those organizations; and

(B) working with countries that are allies or partners of the United States to ensure that foreign adversaries (as defined in section 8(c)(2) of the Secure and Trusted Communications Networks Act of 2019 (47 U.S.C. 1607(c)(2))) do not benefit from United States efforts to increase such investment.

SEC. 8005. REPORT ON INCREASING FOREIGN DIRECT INVESTMENT IN SEMICONDUCTOR-RELATED MANUFACTURING AND PRODUCTION.

Not later than 2 years after the date of the enactment of this Act, the Executive Director of SelectUSA, in coordination with the Federal Interagency Investment Working Group established by Executive Order 13577 (76 Fed. Reg. 35,715; relating to establishment of the SelectUSA Initiative), shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Energy and Commerce of the House of Representatives a report that includes—

(1) a review of the comments SelectUSA received from State-level economic development organizations under section 8004;

(2) a description of activities SelectUSA is engaged in to increase foreign direct investment in semiconductor-related manufacturing and production; and

(3) an assessment of strategies SelectUSA may implement to achieve an increase in such investment and to help secure the United States supply chain for semiconductors, including by—

(A) working with other relevant Federal agencies; and

(B) working with State-level economic development organizations and implementing any strategies or recommendations SelectUSA received from those organizations.

SEC. 8006. NO ADDITIONAL FUNDS.

No additional funds are authorized to be appropriated for the purpose of carrying out this title. The Executive Director of SelectUSA shall carry out this title using amounts otherwise available to the Executive Director for such purposes.

DIVISION I—ENVIRONMENT AND PUBLIC WORKS

SEC. 9001. ACCELERATING DEPLOYMENT OF VERSATILE, ADVANCED NUCLEAR FOR CLEAN ENERGY.

(a) SHORT TITLE.—This section may be cited as the ''Accelerating Deployment of Versatile, Advanced Nuclear for Clean Energy Act of 2023'' or the ''ADVANCE Act of 2023''.

(b) DEFINITIONS.—In this section:

(1) ACCIDENT TOLERANT FUEL.—The term ''accident tolerant fuel'' has the meaning given the term in section 107(a) of the Nuclear Energy Innovation and Modernization Act (Public Law 115–439; 132 Stat. 5577).

(2) ADMINISTRATOR.—The term ''Administrator'' means the Administrator of the Environmental Protection Agency.

(3) ADVANCED NUCLEAR FUEL.—The term ''advanced nuclear fuel'' means—

(A) advanced nuclear reactor fuel; and

(B) accident tolerant fuel.

(4) ADVANCED NUCLEAR REACTOR.—The term ''advanced nuclear reactor'' has the meaning given the term in section 3 of the Nuclear Energy Innovation and Modernization Act (42 U.S.C. 2215 note; Public Law 115–439).

(5) ADVANCED NUCLEAR REACTOR FUEL.—The term ''advanced nuclear reactor fuel'' has the meaning given the term in section 3 of the Nuclear Energy Innovation and Modernization Act (42 U.S.C. 2215 note; Public Law 115–439).

(6) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

(A) the Committee on Environment and Public Works of the Senate; and

(B) the Committee on Energy and Commerce of the House of Representatives.

(7) COMMISSION.—The term ''Commission'' means the Nuclear Regulatory Commission.

(8) INSTITUTION OF HIGHER EDUCATION.—The term ''institution of higher education'' has the meaning given the term in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a)).

(9) NATIONAL LABORATORY.—The term ''National Laboratory'' has the meaning given the term in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801).

(c) INTERNATIONAL NUCLEAR REACTOR EXPORT AND INNOVATION ACTIVITIES.—

(1) COORDINATION.—

(A) IN GENERAL.—The Commission shall—

(i) coordinate all work of the Commission relating to—

(I) nuclear reactor import and export licensing; and

(II) international regulatory cooperation and assistance relating to nuclear reactors, including with countries that are members of—

(aa) the Organisation for Economic Co-operation and Development; or

(bb) the Nuclear Energy Agency; and

(ii) support interagency and international coordination with respect to—

(I) the consideration of international technical standards to establish the licensing and regulatory basis to assist the design, construction, and operation of nuclear systems;

(II) efforts to help build competent nuclear regulatory organizations and legal frameworks in countries seeking to develop nuclear power; and

(III) exchange programs and training provided to other countries relating to nuclear regulation and oversight to improve nuclear technology licensing, in accordance with subparagraph (B).

(B) EXCHANGE PROGRAMS AND TRAINING.—With respect to the exchange programs and training described in subparagraph (A)(ii)(III), the Commission shall coordinate, as applicable, with—

(i) the Secretary of Energy;

(ii) National Laboratories;

(iii) the private sector; and

(iv) institutions of higher education.

(2) AUTHORITY TO ESTABLISH BRANCH.—The Commission may establish within the Office of International Programs a branch, to be known as the ''International Nuclear Reactor Export and Innovation Branch'', to carry out such international nuclear reactor export and innovation activities as the Commission determines to be appropriate and within the mission of the Commission.

(3) EXCLUSION OF INTERNATIONAL ACTIVITIES FROM THE FEE BASE.—

(A) IN GENERAL.—Section 102 of the Nuclear Energy Innovation and Modernization Act (42 U.S.C. 2215) is amended—

(i) in subsection (a), by adding at the end the following:

''(A) INTERNATIONAL NUCLEAR REACTOR EXPORT AND INNOVATION ACTIVITIES.—The Commission shall identify in the annual budget justification international nuclear reactor export and innovation activities described in subsection (c)(1) of the ADVANCE Act of 2023.''; and

(ii) in subsection (b)(1)(B), by adding at the end the following:

''(I) Costs for international nuclear reactor export and innovation activities described in subsection (c)(1) of the ADVANCE Act of 2023.''.

(B) EFFECTIVE DATE.—The amendments made by subparagraph (A) shall take effect on October 1, 2024.

(4) SAVINGS CLAUSE.—Nothing in this subsection alters the authority of the Commission to license and regulate the civilian use of radioactive materials.

(d) DENIAL OF CERTAIN DOMESTIC LICENSES FOR NATIONAL SECURITY PURPOSES.—

(1) DEFINITION OF COVERED FUEL.—In this subsection, the term ''covered fuel'' means enriched uranium that is fabricated into fuel assemblies for nuclear reactors by an entity that—

(A) is owned or controlled by the Government of the Russian Federation or the Government of the People's Republic of China; or

(B) is organized under the laws of, or otherwise subject to the jurisdiction of, the Russian Federation or the People's Republic of China.

(2) PROHIBITION ON UNLICENSED POSSESSION OR OWNERSHIP OF COVERED FUEL.—Unless specifically authorized by the Commission in a license issued under section 53 of the Atomic Energy Act of 1954 (42 U.S.C. 2073) and part 70 of title 10, Code of Federal Regulations (or successor regulations), no person subject to the jurisdiction of the Commission may possess or own covered fuel.

(3) LICENSE TO POSSESS OR OWN COVERED FUEL.—

(A) CONSULTATION REQUIRED PRIOR TO ISSUANCE.—The Commission shall not issue a license to possess or own covered fuel under section 53 of the Atomic Energy Act of 1954 (42 U.S.C. 2073) and part 70 of title 10, Code of Federal Regulations (or successor regulations), unless the Commission has first consulted with the Secretary of Energy and the Secretary of State before issuing the license.

(B) PROHIBITION ON ISSUANCE OF LICENSE.—

(i) IN GENERAL.—Subject to clause (iii), a license to possess or own covered fuel shall not be issued if the Secretary of Energy and the Secretary of State make the determination described in clause (ii).

(ii) DETERMINATION.—

(I) IN GENERAL.—The determination referred to in clause (i) is a determination that possession or ownership, as applicable, of covered fuel poses a threat to the national security of the United States that adversely impacts the physical and economic security of the United States.

(II) JOINT DETERMINATION.—A determination described in subclause (I) shall be jointly made by the Secretary of Energy and the Secretary of State.

(III) TIMELINE.—

(aa) NOTICE OF APPLICATION.—Not later than 30 days after the date on which the Commission receives an application for a license to possess or own covered fuel, the Commission shall notify the Secretary of Energy and the Secretary of State of the application.

(bb) DETERMINATION.—The Secretary of Energy and the Secretary of State shall have a period of 180 days, beginning on the date on which the Commission notifies the Secretary of Energy and the Secretary of State under item (aa) of an application for a license to possess or own covered fuel, in which to make the determination described in subclause (I).

(cc) COMMISSION NOTIFICATION.—On making the determination described in subclause (I), the Secretary of Energy and the Secretary of State shall immediately notify the Commission.

(dd) CONGRESSIONAL NOTIFICATION.—Not later than 30 days after the date on which the Secretary of Energy and the Secretary of State notify the Commission under item (cc), the Commission shall notify the appropriate committees of Congress of the determination.

(ee) PUBLIC NOTICE.—Not later than 15 days after the date on which the Commission notifies Congress under item (dd) of a determination made under subclause (I), the Commission shall make that determination publicly available.

(iii) EFFECT OF NO DETERMINATION.—The prohibition described in clause (i) shall not apply if the Secretary of Energy and the Secretary of State do not make the determination described in clause (ii) by the date described in subclause (III)(bb) of that clause.

(4) SAVINGS CLAUSE.—Nothing in this subsection alters any treaty or international agreement in effect on the date of enactment of this Act.

(e) EXPORT LICENSE REQUIREMENTS.—

(1) DEFINITION OF LOW-ENRICHED URANIUM.—In this subsection, the term ''low-enriched uranium'' means uranium enriched to less than 20 percent of the uranium-235 isotope.

(2) REQUIREMENT.—The Commission shall not issue an export license for the transfer of any item described in paragraph (4) to a country described in paragraph (3) unless the Commission makes a determination that such transfer will not be inimical to the common defense and security of the United States.

(3) COUNTRIES DESCRIBED.—A country referred to in paragraph (2) is a country that—

(A) has not concluded and ratified an Additional Protocol to its safeguards agreement with the International Atomic Energy Agency; or

(B) has not ratified or acceded to the amendment to the Convention on the Physical Protection of Nuclear Material, adopted at Vienna October 26, 1979, and opened for signature at New York March 3, 1980 (TIAS 11080), described in the information circular of the International Atomic Energy Agency numbered INFCIRC/274/Rev.1/Mod.1 and dated May 9, 2016 (TIAS 16–508).

(4) ITEMS DESCRIBED.—An item referred to in paragraph (2) includes—

(A) unirradiated nuclear fuel containing special nuclear material (as defined in section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014)), excluding low-enriched uranium;

(B) a nuclear reactor that uses nuclear fuel described in subparagraph (A); and

(C) any plant or component listed in Appendix I to part 110 of title 10, Code of Federal Regulations (or successor regulations), that is involved in—

(i) the reprocessing of irradiated nuclear reactor fuel elements;

(ii) the separation of plutonium; or

(iii) the separation of the uranium-233 isotope.

(5) NOTIFICATION.—If the Commission makes a determination under paragraph (2) that the transfer of any item described in paragraph (4) to a country described in paragraph (3) will not be inimical to the common defense and security of the United States, the Commission shall notify the appropriate committees of Congress.

(f) COORDINATED INTERNATIONAL ENGAGEMENT.—

(1) DEFINITIONS.—In this subsection:

(A) EMBARKING CIVIL NUCLEAR NATION.—

(i) IN GENERAL.—The term ''embarking civil nuclear nation'' means a country that—

(I) does not have a civil nuclear program;

(II) is in the process of developing or expanding a civil nuclear program, including safeguards and a legal and regulatory framework; or

(III) is in the process of selecting, developing, constructing, or utilizing an advanced nuclear reactor or advanced civil nuclear technologies.

(ii) EXCLUSIONS.—The term ''embarking civil nuclear nation'' does not include—

(I) the People's Republic of China;

(II) the Russian Federation;

(III) the Republic of Belarus;

(IV) the Islamic Republic of Iran;

(V) the Democratic People's Republic of Korea;

(VI) the Republic of Cuba;

(VII) the Bolivarian Republic of Venezuela;

(VIII) the Syrian Arab Republic;

(IX) Burma; or

(X) any other country—

(aa) the property or interests in property of the government of which are blocked pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.); or

(bb) the government of which the Secretary of State has determined has repeatedly provided support for acts of international terrorism for purposes of—

(AA) section 620A(a) of the Foreign Assistance Act of 1961 (22 U.S.C. 2371(a));

(BB) section 40(d) of the Arms Export Control Act (22 U.S.C. 2780(d));

(CC) section 1754(c)(1)(A)(i) of the Export Control Reform Act of 2018 (50 U.S.C. 4813(c)(1)(A)(i)); or

(DD) any other relevant provision of law.

(B) SECRETARIES.—The term ''Secretaries'' means the Secretary of Commerce and the Secretary of Energy, acting—

(i) in consultation with each other; and

(ii) in coordination with—

(I) the Secretary of State;

(II) the Commission;

(III) the Secretary of the Treasury;

(IV) the President of the Export-Import Bank of the United States; and

(V) officials of other Federal agencies, as the Secretary of Commerce determines to be appropriate.

(C) U.S. NUCLEAR ENERGY COMPANY.—The term ''U.S. nuclear energy company'' means a company that—

(i) is organized under the laws of, or otherwise subject to the jurisdiction of, the United States; and

(ii) is involved in the nuclear energy industry.

(2) INTERNATIONAL CIVIL NUCLEAR MODERNIZATION INITIATIVE.—

(A) IN GENERAL.—The Secretaries shall establish and carry out, in accordance with applicable nuclear technology export laws (including regulations), an international initiative to modernize civil nuclear outreach to embarking civil nuclear nations.

(B) ACTIVITIES.—In carrying out the initiative described in subparagraph (A)—

(i) the Secretary of Commerce shall—

(I) expand outreach by the Executive Branch to the private investment community to create public-private financing relationships to assist in the export of civil nuclear technology to embarking civil nuclear nations;

(II) seek to coordinate, to the maximum extent practicable, the work carried out by each of—

(aa) the Commission;

(bb) the Department of Energy;

(cc) the Department of State;

(dd) the Nuclear Energy Agency;

(ee) the International Atomic Energy Agency; and

(ff) other agencies, as the Secretary of Commerce determines to be appropriate; and

(III) improve the regulatory framework to allow for the efficient and expeditious exporting and importing of items under the jurisdiction of the Secretary of Commerce; and

(ii) the Secretary of Energy shall—

(I) assist nongovernmental organizations and appropriate offices, administrations, agencies, laboratories, and programs of the Federal Government in providing education and training to foreign governments in nuclear safety, security, and safeguards—

(aa) through engagement with the International Atomic Energy Agency; or

(bb) independently, if the applicable nongovernmental organization, office, administration, agency, laboratory, or program determines that it would be more advantageous under the circumstances to provide the applicable education and training independently;

(II) assist the efforts of the International Atomic Energy Agency to expand the support provided by the International Atomic Energy Agency to embarking civil nuclear nations for nuclear safety, security, and safeguards; and

(III) assist U.S. nuclear energy companies to integrate security and safeguards by design in international outreach carried out by those U.S. nuclear energy companies.

(3) REPORT.—Not later than 2 years after the date of enactment of this Act, the Secretary of Commerce, in consultation with the Secretary of Energy, shall submit to Congress a report describing the activities carried out under this subsection.

(g) FEES FOR ADVANCED NUCLEAR REACTOR APPLICATION REVIEW.—

(1) DEFINITIONS.—Section 3 of the Nuclear Energy Innovation and Modernization Act (42 U.S.C. 2215 note; Public Law 115–439) is amended—

(A) by redesignating paragraphs (2) through (15) as paragraphs (3), (6), (7), (8), (9), (10), (12), (15), (16), (17), (18), (19), (20), and (21), respectively;

(B) by inserting after paragraph (1) the following:

''(2) ADVANCED NUCLEAR REACTOR APPLICANT.—The term 'advanced nuclear reactor applicant' means an entity that has submitted to the Commission an application to receive a license for an advanced nuclear reactor under the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.).'';

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

''(4) ADVANCED NUCLEAR REACTOR PRE-APPLICANT.—The term 'advanced nuclear reactor pre-applicant' means an entity that has submitted to the Commission a licensing project plan for the purposes of submitting a future application to receive a license for an advanced nuclear reactor under the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.).

''(5) AGENCY SUPPORT.—The term 'agency support' means the resources of the Commission that are located in executive, administrative, and other support offices of the Commission, as described in the document of the Commission entitled 'FY 2023 Final Fee Rule Work Papers' (or a successor document).'';

(D) by inserting after paragraph (10) (as so redesignated) the following:

''(11) HOURLY RATE FOR MISSION-DIRECT PROGRAM SALARIES AND BENEFITS FOR THE NUCLEAR REACTOR SAFETY PROGRAM.—The term 'hourly rate for mission-direct program salaries and benefits for the Nuclear Reactor Safety Program' means the quotient obtained by dividing—

''(A) the full-time equivalent rate (within the meaning of the document of the Commission entitled 'FY 2023 Final Fee Rule Work Papers' (or a successor document)) for mission-direct program salaries and benefits for the Nuclear Reactor Safety Program (as determined by the Commission) for a fiscal year; by

''(B) the productive hours assumption for that fiscal year, determined in accordance with the formula established in the document referred to in subparagraph (A) (or a successor document).''; and

(E) by inserting after paragraph (12) (as so redesignated) the following:

''(13) MISSION-DIRECT PROGRAM SALARIES AND BENEFITS FOR THE NUCLEAR REACTOR SAFETY PROGRAM.—The term 'mission-direct program salaries and benefits for the Nuclear Reactor Safety Program' means the resources of the Commission that are allocated to the Nuclear Reactor Safety Program (as determined by the Commission) to perform core work activities committed to fulfilling the mission of the Commission, as described in the document of the Commission entitled 'FY 2023 Final Fee Rule Work Papers' (or a successor document).

''(14) MISSION-INDIRECT PROGRAM SUPPORT.—The term 'mission-indirect program support' means the resources of the Commission that support the core mission-direct activities for the Nuclear Reactor Safety Program of the Commission (as determined by the Commission), as described in the document of the Commission entitled 'FY 2023 Final Fee Rule Work Papers' (or a successor document).''.

(2) EXCLUDED ACTIVITIES.—Section 102(b)(1)(B) of the Nuclear Energy Innovation and Modernization Act (42 U.S.C. 2215(b)(1)(B)) (as amended by subsection (c)(3)(A)(ii)) is amended by adding at the end the following:

''(v) The total costs of mission-indirect program support and agency support that, under paragraph (2)(B), may not be included in the hourly rate charged for fees assessed to advanced nuclear reactor applicants.

''(vi) The total costs of mission-indirect program support and agency support that, under paragraph (2)(C), may not be included in the hourly rate charged for fees assessed to advanced nuclear reactor pre-applicants.''.

(3) FEES FOR SERVICE OR THING OF VALUE.—Section 102(b) of the Nuclear Energy Innovation and Modernization Act (42 U.S.C. 2215(b)) is amended by striking paragraph (2) and inserting the following:

''(2) FEES FOR SERVICE OR THING OF VALUE.—

''(A) IN GENERAL.—In accordance with section 9701 of title 31, United States Code, the Commission shall assess and collect fees from any person who receives a service or

thing of value from the Commission to cover the costs to the Commission of providing the service or thing of value.

''(B) ADVANCED NUCLEAR REACTOR APPLICANTS.—The hourly rate charged for fees assessed to advanced nuclear reactor applicants under this paragraph relating to the review of a submitted application described in section 3(1) shall not exceed the hourly rate for mission-direct program salaries and benefits for the Nuclear Reactor Safety Program.

''(C) ADVANCED NUCLEAR REACTOR PRE-APPLICANTS.—The hourly rate charged for fees assessed to advanced nuclear reactor pre-applicants under this paragraph relating to the review of submitted materials as described in the licensing project plan of an advanced nuclear reactor pre-applicant shall not exceed the hourly rate for mission-direct program salaries and benefits for the Nuclear Reactor Safety Program.''.

(4) SUNSET.—Section 102 of the Nuclear Energy Innovation and Modernization Act (42 U.S.C. 2215) is amended by adding at the end the following:

''(g) CESSATION OF EFFECTIVENESS.—Paragraphs (1)(B)(vi) and (2)(C) of subsection (b) shall cease to be effective on September 30, 2029.''.

(5) EFFECTIVE DATE.—The amendments made by this subsection shall take effect on October 1, 2024.

(h) ADVANCED NUCLEAR REACTOR PRIZES.—Section 103 of the Nuclear Energy Innovation and Modernization Act (Public Law 115–439; 132 Stat. 5571) is amended by adding at the end the following:

''(f) PRIZES FOR ADVANCED NUCLEAR REACTOR LICENSING.—

''(1) DEFINITION OF ELIGIBLE ENTITY.—In this subsection, the term 'eligible entity' means—

''(A) a non-Federal entity; and

''(B) the Tennessee Valley Authority.

''(2) PRIZE FOR ADVANCED NUCLEAR REACTOR LICENSING.—

''(A) IN GENERAL.—Notwithstanding section 169 of the Atomic Energy Act of 1954 (42 U.S.C. 2209) and subject to the availability of appropriations, the Secretary is authorized to make, with respect to each award category described in subparagraph (C), an award in an amount described in subparagraph (B) to the first eligible entity—

''(i) to which the Commission issues an operating license for an advanced nuclear reactor under part 50 of title 10, Code of Federal Regulations (or successor regulations), for which an application has not been approved by the Commission as of the date of enactment of this subsection; or

''(ii) for which the Commission makes a finding described in section 52.103(g) of title 10, Code of Federal Regulations (or successor regulations), with respect to a combined license for an advanced nuclear reactor—

''(I) that is issued under subpart C of part 52 of that title (or successor regulations); and

''(II) for which an application has not been approved by the Commission as of the date of enactment of this subsection.

''(B) AMOUNT OF AWARD.—An award under subparagraph (A) shall be in an amount equal to the total amount assessed by the Commission and collected under section 102(b)(2) from the eligible entity receiving the award for costs relating to the issuance of the license described in that subparagraph, including, as applicable, costs relating to the issuance of an associated construction permit described in section 50.23 of title 10, Code of Federal Regulations (or successor regulations), or early site permit (as defined in section 52.1 of that title (or successor regulations)).

''(C) AWARD CATEGORIES.—An award under subparagraph (A) may be made for—

''(i) the first advanced nuclear reactor for which the Commission—

''(I) issues a license in accordance with clause (i) of subparagraph (A); or

''(II) makes a finding in accordance with clause (ii) of that subparagraph;

''(ii) an advanced nuclear reactor that—

''(I) uses isotopes derived from spent nuclear fuel (as defined in section 2 of the Nuclear Waste Policy Act of 1982 (42 U.S.C. 10101)) or depleted uranium as fuel for the advanced nuclear reactor; and

''(II) is the first advanced nuclear reactor described in subclause (I) for which the Commission—

''(aa) issues a license in accordance with clause (i) of subparagraph (A); or

''(bb) makes a finding in accordance with clause (ii) of that subparagraph;

''(iii) an advanced nuclear reactor that—

''(I) is a nuclear integrated energy system—

''(aa) that is composed of 2 or more co-located or jointly operated subsystems of energy generation, energy storage, or other technologies;

''(bb) in which not fewer than 1 subsystem described in item (aa) is a nuclear energy system; and

''(cc) the purpose of which is—

''(AA) to reduce greenhouse gas emissions in both the power and nonpower sectors; and

''(BB) to maximize energy production and efficiency; and

''(II) is the first advanced nuclear reactor described in subclause (I) for which the Commission—

''(aa) issues a license in accordance with clause (i) of subparagraph (A); or

''(bb) makes a finding in accordance with clause (ii) of that subparagraph;

''(iv) an advanced reactor that—

''(I) operates flexibly to generate electricity or high temperature process heat for nonelectric applications; and

''(II) is the first advanced nuclear reactor described in subclause (I) for which the Commission—

''(aa) issues a license in accordance with clause (i) of subparagraph (A); or

''(bb) makes a finding in accordance with clause (ii) of that subparagraph; and

''(v) the first advanced nuclear reactor for which the Commission grants approval to load nuclear fuel pursuant to the technology-inclusive regulatory framework established under subsection (a)(4).

''(3) FEDERAL FUNDING LIMITATIONS.—

''(A) EXCLUSION OF TVA FUNDS.—In this paragraph, the term 'Federal funds' does not include funds received under the power program of the Tennessee Valley Authority.

''(B) LIMITATION ON AMOUNTS EXPENDED.—An award under this subsection shall not exceed the total amount expended (excluding any expenditures made with Federal funds received for the applicable project and an amount equal to the minimum cost-share required under section 988 of the Energy Policy Act of 2005 (42 U.S.C. 16352)) by the eligible entity receiving the award for licensing costs relating to the project for which the award is made.

''(C) REPAYMENT AND DIVIDENDS NOT REQUIRED.—Notwithstanding section 9104(a)(4) of title 31, United States Code, or any other provision of law, an eligible entity that receives an award under this subsection shall not be required—

''(i) to repay that award or any part of that award; or

''(ii) to pay a dividend, interest, or other similar payment based on the sum of that award.''.

(i) REPORT ON UNIQUE LICENSING CONSIDERATIONS RELATING TO THE USE OF NUCLEAR ENERGY FOR NONELECTRIC APPLICATIONS.—

(1) IN GENERAL.—Not later than 270 days after the date of enactment of this Act, the Commission shall submit to the appropriate committees of Congress a report (referred to in this subsection as the ''report'') addressing any unique licensing issues or requirements relating to—

(A) the flexible operation of nuclear reactors, such as ramping power output and switching between electricity generation and nonelectric applications;

(B) the use of advanced nuclear reactors exclusively for nonelectric applications; and

(C) the colocation of nuclear reactors with industrial plants or other facilities.

(2) STAKEHOLDER INPUT.—In developing the report, the Commission shall seek input from—

(A) the Secretary of Energy;

(B) the nuclear energy industry;

(C) technology developers;

(D) the industrial, chemical, and medical sectors;

(E) nongovernmental organizations; and

(F) other public stakeholders.

(3) CONTENTS.—

(A) IN GENERAL.—The report shall describe—

(i) any unique licensing issues or requirements relating to the matters described in subparagraphs (A) through (C) of paragraph (1), including, with respect to the nonelectric applications referred to in subparagraphs (A) and (B) of that paragraph, any licensing issues or requirements relating to the use of nuclear energy in—

(I) hydrogen or other liquid and gaseous fuel or chemical production;

(II) water desalination and wastewater treatment;

(III) heat for industrial processes;

(IV) district heating;

(V) energy storage;

(VI) industrial or medical isotope production; and

(VII) other applications, as identified by the Commission;

(ii) options for addressing those issues or requirements—

(I) within the existing regulatory framework of the Commission;

(II) as part of the technology-inclusive regulatory framework required under subsection (a)(4) of section 103 of the Nuclear Energy Innovation and Modernization Act (42 U.S.C. 2133 note; Public Law 115–439) or described in the report required under subsection (e) of that section (Public Law 115–439; 132 Stat. 5575); or

(III) through a new rulemaking; and

(iii) the extent to which Commission action is needed to implement any matter described in the report.

(B) COST ESTIMATES, BUDGETS, AND TIMEFRAMES.—The report shall include cost estimates, proposed budgets, and proposed timeframes for implementing risk-informed and performance-based regulatory guidance in the licensing of nuclear reactors for nonelectric applications.

(j) ENABLING PREPARATIONS FOR THE DEMONSTRATION OF ADVANCED NUCLEAR REACTORS ON DEPARTMENT OF ENERGY SITES OR CRITICAL NATIONAL SECURITY INFRASTRUCTURE SITES.—

(1) IN GENERAL.—Section 102(b)(1)(B) of the Nuclear Energy Innovation and Modernization Act (42 U.S.C. 2215(b)(1)(B)) (as amended by subsection (g)(2)) is amended by adding at the end the following:

''(vi) Costs for—

''(I) activities to review and approve or disapprove an application for an early site permit (as defined in section 52.1 of title 10, Code of Federal Regulations (or a successor

regulation)) to demonstrate an advanced nuclear reactor on a Department of Energy site or critical national security infrastructure (as defined in section 327(d) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 132 Stat. 1722)) site; and

''(II) pre-application activities relating to an early site permit (as defined in section 52.1 of title 10, Code of Federal Regulations (or a successor regulation)) to demonstrate an advanced nuclear reactor on a Department of Energy site or critical national security infrastructure (as defined in section 327(d) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 132 Stat. 1722)) site.''.

(2) EFFECTIVE DATE.—The amendment made by paragraph (1) shall take effect on October 1, 2024.

(k) CLARIFICATION ON FUSION REGULATION.—Section 103(a)(4) of the Nuclear Energy Innovation and Modernization Act (42 U.S.C. 2133 note; Public Law 115–439) is amended—

(1) by striking ''Not later'' and inserting the following:

''(A) IN GENERAL.—Not later''; and

(2) by adding at the end the following:

''(B) EXCLUSION OF FUSION REACTORS.—For purposes of subparagraph (A), the term 'advanced reactor applicant' does not include an applicant seeking a license for a fusion reactor.''.

(l) REGULATORY ISSUES FOR NUCLEAR FACILITIES AT BROWNFIELD SITES.—

(1) DEFINITIONS.—

(A) BROWNFIELD SITE.—The term ''brownfield site'' has the meaning given the term in section 101 of the Comprehensive Environmental Response, Compensation, and Liability Act of 1980 (42 U.S.C. 9601).

(B) PRODUCTION FACILITY.—The term ''production facility'' has the meaning given the term in section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014).

(C) RETIRED FOSSIL FUEL SITE.—The term ''retired fossil fuel site'' means the site of 1 or more fossil fuel electric generation facilities that are retired or scheduled to retire, including multi-unit facilities that are partially shut down.

(D) UTILIZATION FACILITY.—The term ''utilization facility'' has the meaning given the term in section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014).

(2) IDENTIFICATION OF REGULATORY ISSUES.—

(A) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Commission shall evaluate the extent to which modification of regulations, guidance, or policy is needed to enable timely licensing reviews for, and to support the oversight of, production facilities or utilization facilities at brownfield sites.

(B) REQUIREMENT.—In carrying out subparagraph (A), the Commission shall consider how licensing reviews for production facilities or utilization facilities at brownfield sites may be expedited by considering matters relating to siting and operating a production facility or a utilization facility at or near a retired fossil fuel site to support—

(i) the reuse of existing site infrastructure, including—

(I) electric switchyard components and transmission infrastructure;

(II) heat-sink components;

(III) steam cycle components;

(IV) roads;

(V) railroad access; and

(VI) water availability;

(ii) the use of early site permits;

(iii) the utilization of plant parameter envelopes or similar standardized site parameters on a portion of a larger site; and

(iv) the use of a standardized application for similar sites.

(C) REPORT.—Not later than 14 months after the date of enactment of this Act, the Commission shall submit to the appropriate committees of Congress a report describing any regulations, guidance, and policies identified under subparagraph (A).

(3) LICENSING.—

(A) IN GENERAL.—Not later than 2 years after the date of enactment of this Act, the Commission shall—

(i) develop and implement strategies to enable timely licensing reviews for, and to support the oversight of, production facilities or utilization facilities at brownfield sites, including retired fossil fuel sites; or

(ii) initiate a rulemaking to enable timely licensing reviews for, and to support the oversight of, of production facilities or utilization facilities at brownfield sites, including retired fossil fuel sites.

(B) REQUIREMENTS.—In carrying out subparagraph (A), consistent with the mission of the Commission, the Commission shall consider matters relating to—

(i) the use of existing site infrastructure;

(ii) existing emergency preparedness organizations and planning;

(iii) the availability of historical site-specific environmental data;

(iv) previously approved environmental reviews required by the National Environmental Policy Act of 1969 (42 U.S.C. 4321 et seq.);

(v) activities associated with the potential decommissioning of facilities or decontamination and remediation at brownfield sites; and

(vi) community engagement and historical experience with energy production.

(4) REPORT.—Not later than 3 years after the date of enactment of this Act, the Commission shall submit to the appropriate committees of Congress a report describing the actions taken by the Commission under paragraph (3).

(m) APPALACHIAN REGIONAL COMMISSION NUCLEAR ENERGY DEVELOPMENT.—

(1) IN GENERAL.—Subchapter I of chapter 145 of subtitle IV of title 40, United States Code, is amended by adding at the end the following:

''§ 14512. Appalachian Regional Commission nuclear energy development

''(a) DEFINITIONS.—In this section:

''(1) BROWNFIELD SITE.—The term 'brownfield site' has the meaning given the term in section 101 of the Comprehensive Environmental Response, Compensation, and Liability Act of 1980 (42 U.S.C. 9601).

''(2) PRODUCTION FACILITY.—The term 'production facility' has the meaning given the term in section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014).

''(3) RETIRED FOSSIL FUEL SITE.—The term 'retired fossil fuel site' means the site of 1 or more fossil fuel electric generation facilities that are retired or scheduled to retire, including multi-unit facilities that are partially shut down.

''(4) UTILIZATION FACILITY.—The term 'utilization facility' has the meaning given the term in section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014).

''(b) AUTHORITY.—The Appalachian Regional Commission may provide technical assistance to, make grants to, enter into contracts with, or otherwise provide amounts to individuals or entities in the Appalachian region for projects and activities—

''(1) to conduct research and analysis regarding the economic impact of siting, constructing, and operating a production facility or a utilization facility at a brownfield site, including a retired fossil fuel site;

''(2) to assist with workforce training or retraining to perform activities relating to the siting and operation of a production facility or a utilization facility at a brownfield site, including a retired fossil fuel site; and

''(3) to engage with the Nuclear Regulatory Commission, the Department of Energy, and other Federal agencies with expertise in civil nuclear energy.

''(c) LIMITATION ON AVAILABLE AMOUNTS.—Of the cost of any project or activity eligible for a grant under this section—

''(1) except as provided in paragraphs (2) and (3), not more than 50 percent may be provided from amounts made available to carry out this section;

''(2) in the case of a project or activity to be carried out in a county for which a distressed county designation is in effect under section 14526, not more than 80 percent may be provided from amounts made available to carry out this section; and

''(3) in the case of a project or activity to be carried out in a county for which an at-risk county designation is in effect under section 14526, not more than 70 percent may be provided from amounts made available to carry out this section.

''(d) SOURCES OF ASSISTANCE.—Subject to subsection (c), a grant provided under this section may be provided from amounts made available to carry out this section, in combination with amounts made available—

''(1) under any other Federal program; or

''(2) from any other source.

''(e) FEDERAL SHARE.—Notwithstanding any provision of law limiting the Federal share under any other Federal program, amounts made available to carry out this section may be used to increase that Federal share, as the Appalachian Regional Commission determines to be appropriate.''.

(2) AUTHORIZATION OF APPROPRIATIONS.—Section 14703 of title 40, United States Code, is amended—

(A) by redesignating subsections (e) and (f) as subsections (f) and (g), respectively; and

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

''(e) APPALACHIAN REGIONAL COMMISSION NUCLEAR ENERGY DEVELOPMENT.—Of the amounts made available under subsection (a), $5,000,000 may be used to carry out section 14512 for each of fiscal years 2023 through 2026.''.

(3) CLERICAL AMENDMENT.—The analysis for subchapter I of chapter 145 of subtitle IV of title 40, United States Code, is amended by striking the item relating to section 14511 and inserting the following:

''14511. Appalachian regional energy hub initiative.

''14512. Appalachian Regional Commission nuclear energy development.''.

(n) INVESTMENT BY ALLIES.—

(1) IN GENERAL.—The prohibitions against issuing certain licenses for utilization facilities to certain corporations and other entities described in the second sentence of section 103 d. of the Atomic Energy Act of 1954 (42 U.S.C. 2133(d)) and the second sentence of section 104 d. of that Act (42 U.S.C. 2134(d)) shall not apply to an entity described in paragraph (2) if the Commission determines that issuance of the applicable license to that entity is not inimical to—

(A) the common defense and security; or

(B) the health and safety of the public.

(2) ENTITIES DESCRIBED.—

(A) IN GENERAL.—An entity referred to in paragraph (1) is a corporation or other entity that is owned, controlled, or dominated by—

(i) the government of—

(I) a country that is a member of the Organisation for Economic Co-operation and Development on the date of enactment of this Act, subject to subparagraph (B); or

(II) the Republic of India;

(ii) a corporation that is incorporated in a country described in subclause (I) or (II) of clause (i); or

(iii) an alien who is a national of a country described in subclause (I) or (II) of clause (i).

(B) EXCLUSION.—An entity described in subparagraph (A)(i)(I) is not an entity referred to in paragraph (1), and paragraph (1) shall not apply to that entity, if, on the date of enactment of this Act—

(i) the entity (or any department, agency, or instrumentality of the entity) is a person subject to sanctions under section 231 of the Countering America's Adversaries Through Sanctions Act (22 U.S.C. 9525); or

(ii) any citizen of the entity, or any entity organized under the laws of, or otherwise subject to the jurisdiction of, the entity, is a person subject to sanctions under that section.

(3) TECHNICAL AMENDMENT.—Section 103 d. of the Atomic Energy Act of 1954 (42 U.S.C. 2133(d)) is amended, in the second sentence, by striking ''any any'' and inserting ''any''.

(4) SAVINGS CLAUSE.—Nothing in this subsection affects the requirements of section 721 of the Defense Production Act of 1950 (50 U.S.C. 4565).

(o) EXTENSION OF THE PRICE-ANDERSON ACT.—

(1) EXTENSION.—Section 170 of the Atomic Energy Act of 1954 (42 U.S.C. 2210) (commonly known as the ''Price-Anderson Act'') is amended by striking ''December 31, 2025'' each place it appears and inserting ''December 31, 2045''.

(2) LIABILITY.—Section 170 of the Atomic Energy Act of 1954 (42 U.S.C. 2210) (commonly known as the ''Price-Anderson Act'') is amended—

(A) in subsection d. (5), by striking ''$500,000,000'' and inserting ''$2,000,000,000''; and

(B) in subsection e. (4), by striking ''$500,000,000'' and inserting ''$2,000,000,000''.

(3) REPORT.—Section 170 p. of the Atomic Energy Act of 1954 (42 U.S.C. 2210(p)) (commonly known as the ''Price-Anderson Act'') is amended by striking ''December 31, 2021'' and inserting ''December 31, 2041''.

(4) DEFINITION OF NUCLEAR INCIDENT.—Section 11 q. of the Atomic Energy Act of 1954 (42 U.S.C. 2014(q)) is amended, in the second proviso, by striking ''if such occurrence'' and all that follows through ''United States:'' and inserting a colon.

(p) REPORT ON ADVANCED METHODS OF MANUFACTURING AND CONSTRUCTION FOR NUCLEAR ENERGY APPLICATIONS.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Commission shall submit to the appropriate committees of Congress a report (referred to in this subsection as the ''report'') on manufacturing and construction for nuclear energy applications.

(2) STAKEHOLDER INPUT.—In developing the report, the Commission shall seek input from—

(A) the Secretary of Energy;

(B) the nuclear energy industry;

(C) National Laboratories;

(D) institutions of higher education;

(E) nuclear and manufacturing technology developers;

(F) the manufacturing and construction industries, including manufacturing and construction companies with operating facilities in the United States;

(G) standards development organizations;

(H) labor unions;

(I) nongovernmental organizations; and

(J) other public stakeholders.

(3) CONTENTS.—

(A) IN GENERAL.—The report shall—

(i) examine any unique licensing issues or requirements relating to the use of innovative—

(I) advanced manufacturing processes;

(II) advanced construction techniques; and

(III) rapid improvement or iterative innovation processes;

(ii) examine—

(I) the requirements for nuclear-grade components in manufacturing and construction for nuclear energy applications;

(II) opportunities to use standard materials, parts, or components in manufacturing and construction for nuclear energy applications;

(III) opportunities to use standard materials that are in compliance with existing codes to provide acceptable approaches to support or encapsulate new materials that do not yet have applicable codes; and

(IV) requirements relating to the transport of a fueled advanced nuclear reactor core from a manufacturing licensee to a licensee that holds a license to construct and operate a facility at a particular site;

(iii) identify any safety aspects of innovative advanced manufacturing processes and advanced construction techniques that are not addressed by existing codes and standards, so that generic guidance may be updated or created, as necessary;

(iv) identify options for addressing the issues, requirements, and opportunities examined under clauses (i) and (ii)—

(I) within the existing regulatory framework; or

(II) through a new rulemaking;

(v) identify how addressing the issues, requirements, and opportunities examined under clauses (i) and (ii) will impact opportunities for domestic nuclear manufacturing and construction developers; and

(vi) describe the extent to which Commission action is needed to implement any matter described in the report.

(B) COST ESTIMATES, BUDGETS, AND TIMEFRAMES.—The report shall include cost estimates, proposed budgets, and proposed timeframes for implementing risk-informed and performance-based regulatory guidance for manufacturing and construction for nuclear energy applications.

(q) NUCLEAR ENERGY TRAINEESHIP.—Section 313 of division C of the Omnibus Appropriations Act, 2009 (42 U.S.C. 16274a), is amended—

(1) in subsection (a), by striking ''Nuclear Regulatory'';

(2) in subsection (b)(1), in the matter preceding subparagraph (A), by inserting ''and subsection (c)'' after ''paragraph (2)'';

(3) in subsection (c)—

(A) by redesignating paragraph (2) as paragraph (5); and

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

''(1) ADVANCED NUCLEAR REACTOR.—The term 'advanced nuclear reactor' has the meaning given the term in section 951(b) of the Energy Policy Act of 2005 (42 U.S.C. 16271(b)).

''(2) COMMISSION.—The term 'Commission' means the Nuclear Regulatory Commission.

''(3) INSTITUTION OF HIGHER EDUCATION.—The term 'institution of higher education' has the meaning given the term in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801).

''(4) NATIONAL LABORATORY.—The term 'National Laboratory' has the meaning given the term in section 951(b) of the Energy Policy Act of 2005 (42 U.S.C. 16271(b)).'';

(4) in subsection (d)(2), by striking ''Nuclear Regulatory'';

(5) by redesignating subsections (c) and (d) as subsections (d) and (e), respectively; and

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

''(c) NUCLEAR ENERGY TRAINEESHIP SUBPROGRAM.—

''(1) IN GENERAL.—The Commission shall establish, as a subprogram of the Program, a nuclear energy traineeship subprogram under which the Commission, in coordination with institutions of higher education and trade schools, shall competitively award traineeships that provide focused training to meet critical mission needs of the Commission and nuclear workforce needs, including needs relating to the nuclear tradecraft workforce.

''(2) REQUIREMENTS.—In carrying out the nuclear energy traineeship subprogram described in paragraph (1), the Commission shall—

''(A) coordinate with the Secretary of Energy to prioritize the funding of traineeships that focus on—

''(i) nuclear workforce needs; and

''(ii) critical mission needs of the Commission;

''(B) encourage appropriate partnerships among—

''(i) National Laboratories;

''(ii) institutions of higher education;

''(iii) trade schools;

''(iv) the nuclear energy industry; and

''(v) other entities, as the Commission determines to be appropriate; and

''(C) on an annual basis, evaluate nuclear workforce needs for the purpose of implementing traineeships in focused topical areas that—

''(i) address the workforce needs of the nuclear energy community; and

''(ii) support critical mission needs of the Commission.''.

(r) REPORT ON COMMISSION READINESS AND CAPACITY TO LICENSE ADDITIONAL CONVERSION AND ENRICHMENT CAPACITY TO REDUCE RELIANCE ON URANIUM FROM RUSSIA.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Commission shall submit to the appropriate committees of Congress a report on the readiness and capacity of the Commission to license additional conversion and enrichment capacity at existing and new fuel cycle facilities to reduce reliance on nuclear fuel that is recovered, converted, enriched, or fabricated by an entity that—

(A) is owned or controlled by the Government of the Russian Federation; or

(B) is organized under the laws of, or otherwise subject to the jurisdiction of, the Russian Federation.

(2) CONTENTS.—The report required under paragraph (1) shall analyze how the capacity of the Commission to license additional conversion and enrichment capacity at existing and new fuel cycle facilities may conflict with or restrict the readiness of the Commission to review advanced nuclear reactor applications.

(s) ANNUAL REPORT ON THE SPENT NUCLEAR FUEL AND HIGH-LEVEL RADIOACTIVE WASTE INVENTORY IN THE UNITED STATES.—

(1) DEFINITIONS.—In this subsection:

(A) HIGH-LEVEL RADIOACTIVE WASTE.—The term ''high-level radioactive waste'' has the meaning given the term in section 2 of the Nuclear Waste Policy Act of 1982 (42 U.S.C. 10101).

(B) SPENT NUCLEAR FUEL.—The term ''spent nuclear fuel'' has the meaning given the term in section 2 of the Nuclear Waste Policy Act of 1982 (42 U.S.C. 10101).

(C) STANDARD CONTRACT.—The term ''standard contract'' has the meaning given the term ''contract'' in section 961.3 of title 10, Code of Federal Regulations (or a successor regulation).

(2) REPORT.—Not later than January 1, 2025, and annually thereafter, the Secretary of Energy shall submit to Congress a report that describes—

(A) the annual and cumulative amount of payments made by the United States to the

holder of a standard contract due to a partial breach of contract under the Nuclear Waste Policy Act of 1982 (42 U.S.C. 10101 et seq.) resulting in financial damages to the holder;

(B) the cumulative amount spent by the Department of Energy since fiscal year 2008 to reduce future payments projected to be made by the United States to any holder of a standard contract due to a partial breach of contract under the Nuclear Waste Policy Act of 1982 (42 U.S.C. 10101 et seq.);

(C) the cumulative amount spent by the Department of Energy to store, manage, and dispose of spent nuclear fuel and high-level radioactive waste in the United States as of the date of the report;

(D) the projected lifecycle costs to store, manage, transport, and dispose of the projected inventory of spent nuclear fuel and high-level radioactive waste in the United States, including spent nuclear fuel and high-level radioactive waste expected to be generated from existing reactors through 2050;

(E) any mechanisms for better accounting of liabilities for the lifecycle costs of the spent nuclear fuel and high-level radioactive waste inventory in the United States;

(F) any recommendations for improving the methods used by the Department of Energy for the accounting of spent nuclear fuel and high-level radioactive waste costs and liabilities;

(G) any actions taken in the previous fiscal year by the Department of Energy with respect to interim storage; and

(H) any activities taken in the previous fiscal year by the Department of Energy to develop and deploy nuclear technologies and fuels that enhance the safe transportation or storage of spent nuclear fuel or high-level radioactive waste, including technologies to protect against seismic, flooding, and other extreme weather events.

(t) AUTHORIZATION OF APPROPRIATIONS FOR SUPERFUND ACTIONS AT ABANDONED MINING SITES ON TRIBAL LAND.—

(1) DEFINITIONS.—In this subsection:

(A) ELIGIBLE NON-NPL SITE.—The term ''eligible non-NPL site'' means a site—

(i) that is not on the National Priorities List; but

(ii) with respect to which the Administrator determines that—

(I) the site would be eligible for listing on the National Priorities List based on the presence of hazards from contamination at the site, applying the hazard ranking system described in section 105(c) of the Comprehensive Environmental Response, Compensation, and Liability Act of 1980 (42 U.S.C. 9605(c)); and

(II) for removal site evaluations, engineering evaluations/cost analyses, remedial planning activities, remedial investigations and feasibility studies, and other actions taken pursuant to section 104(b) of that Act (42 U.S.C. 9604), the site—

(aa) has undergone a pre-CERCLA screening; and

(bb) is included in the Superfund Enterprise Management System.

(B) INDIAN TRIBE.—The term ''Indian Tribe'' has the meaning given the term in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 5304).

(C) NATIONAL PRIORITIES LIST.—The term ''National Priorities List'' means the National Priorities List developed by the President in accordance with section 105(a)(8)(B) of the Comprehensive Environmental Response, Compensation, and Liability Act of 1980 (42 U.S.C. 9605(a)(8)(B)).

(D) REMEDIAL ACTION; REMOVAL; RESPONSE.—The terms ''remedial action'', ''removal'', and ''response'' have the meanings given those terms in section 101 of the Comprehensive Environmental Response, Compensation, and Liability Act of 1980 (42 U.S.C. 9601).

(E) TRIBAL LAND.—The term ''Tribal land'' has the meaning given the term ''Indian country'' in section 1151 of title 18, United States Code.

(2) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for each of fiscal years 2023 through 2032, to remain available until expended—

(A) $97,000,000 to the Administrator to carry out this subsection (except for paragraph (4)); and

(B) $3,000,000 to the Administrator of the Agency for Toxic Substances and Disease Registry to carry out paragraph (4).

(3) USES OF AMOUNTS.—Amounts appropriated under paragraph (2)(A) shall be used by the Administrator—

(A) to carry out removal actions on abandoned mine land located on Tribal land;

(B) to carry out response actions, including removal and remedial planning activities, removal and remedial studies, remedial actions, and other actions taken pursuant to section 104(b) of the Comprehensive Environmental Response, Compensation, and Liability Act of 1980 (42 U.S.C. 9604(b)) on abandoned mine land located on Tribal land at—

(i) eligible non-NPL sites; and

(ii) sites listed on the National Priorities List; and

(C) to make grants under paragraph (5).

(4) HEALTH ASSESSMENTS.—Subject to the availability of appropriations, the Agency for Toxic Substances and Disease Registry, in coordination with Tribal health authorities, shall perform 1 or more health assessments at each eligible non-NPL site that is located on Tribal land, in accordance with section 104(i)(6) of the Comprehensive Environmental Response, Compensation, and Liability Act of 1980 (42 U.S.C. 9604(i)(6)).

(5) TRIBAL GRANTS.—

(A) IN GENERAL.—The Administrator may use amounts appropriated under paragraph (2)(A) to make grants to eligible entities described in subparagraph (B) for the purposes described in subparagraph (C).

(B) ELIGIBLE ENTITIES DESCRIBED.—An eligible entity referred to in subparagraph (A) is—

(i) the governing body of an Indian Tribe; or

(ii) a legally established organization of Indians that—

(I) is controlled, sanctioned, or chartered by the governing bodies of 2 or more Indian Tribes to be served, or that is democratically elected by the adult members of the Indian community to be served, by that organization; and

(II) includes the maximum participation of Indians in all phases of the activities of that organization.

(C) USE OF GRANT FUNDS.—A grant under this paragraph shall be used—

(i) in accordance with the second sentence of section 117(e)(1) of the Comprehensive Environmental Response, Compensation, and Liability Act of 1980 (42 U.S.C. 9617(e)(1));

(ii) for obtaining technical assistance in carrying out response actions under clause (iii); or

(iii) for carrying out response actions, if the Administrator determines that the Indian Tribe has the capability to carry out any or all of those response actions in accordance with the criteria and priorities established pursuant to section 105(a)(8) of the Comprehensive Environmental Response, Compensation, and Liability Act of 1980 (42 U.S.C. 9605(a)(8)).

(D) APPLICATIONS.—An eligible entity desiring a grant under this paragraph shall submit to the Administrator an application at such time, in such manner, and containing such information as the Administrator may require.

(E) LIMITATIONS.—A grant under this paragraph shall be governed by the rules, procedures, and limitations described in section 117(e)(2) of the Comprehensive Environmental Response, Compensation, and Liability Act of 1980 (42 U.S.C. 9617(e)(2)), except that—

(i) ''Administrator of the Environmental Protection Agency'' shall be substituted for ''President'' each place it appears in that section; and

(ii) in the first sentence of that section, ''under subsection (t) of the ADVANCE Act of 2023'' shall be substituted for ''under this subsection''.

(6) STATUTE OF LIMITATIONS.—If a remedial action described in paragraph (3)(B) is scheduled at an eligible non-NPL site, no action may be commenced for damages (as defined in section 101 of the Comprehensive Environmental Response, Compensation, and Liability Act of 1980 (42 U.S.C. 9601)) with respect to that eligible non-NPL site unless the action is commenced within the timeframe provided for such actions with respect to facilities on the National Priorities List in the first sentence of the matter following subparagraph (B) of section 113(g)(1) of that Act (42 U.S.C. 9613(g)(1)).

(7) COORDINATION.—The Administrator shall coordinate with the Indian Tribe on whose land the applicable site is located in—

(A) selecting and prioritizing sites for response actions under subparagraphs (A) and (B) of paragraph (3); and

(B) carrying out those response actions.

(u) DEVELOPMENT, QUALIFICATION, AND LICENSING OF ADVANCED NUCLEAR FUEL CONCEPTS.—

(1) IN GENERAL.—The Commission shall establish an initiative to enhance preparedness and coordination with respect to the qualification and licensing of advanced nuclear fuel.

(2) AGENCY COORDINATION.—Not later than 180 days after the date of enactment of this Act, the Commission and the Secretary of Energy shall enter into a memorandum of understanding—

(A) to share technical expertise and knowledge through—

(i) enabling the testing and demonstration of accident tolerant fuels for existing commercial nuclear reactors and advanced nuclear reactor fuel concepts to be proposed and funded, in whole or in part, by the private sector;

(ii) operating a database to store and share data and knowledge relevant to nuclear science and engineering between Federal agencies and the private sector;

(iii) leveraging expertise with respect to safety analysis and research relating to advanced nuclear fuel; and

(iv) enabling technical staff to actively observe and learn about technologies, with an emphasis on identification of additional information needed with respect to advanced nuclear fuel; and

(B) to ensure that—

(i) the Department of Energy has sufficient technical expertise to support the timely research, development, demonstration, and commercial application of advanced nuclear fuel;

(ii) the Commission has sufficient technical expertise to support the evaluation of applications for licenses, permits, and design certifications and other requests for regulatory approval for advanced nuclear fuel;

(iii)(I) the Department of Energy maintains and develops the facilities necessary to enable the timely research, development, demonstration, and commercial application by the civilian nuclear industry of advanced nuclear fuel; and

(II) the Commission has access to the facilities described in subclause (I), as needed; and

(iv) the Commission consults, as appropriate, with the modeling and simulation experts at the Office of Nuclear Energy of the Department of Energy, at the National Laboratories, and within industry fuel vendor teams in cooperative agreements with the Department of Energy to leverage physics-based computer modeling and simulation capabilities.

(3) REPORT.—

(A) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Commission shall submit to the appropriate committees of Congress a report describing the efforts of the Commission under paragraph (1), including—

(i) an assessment of the preparedness of the Commission to review and qualify for use—

(I) accident tolerant fuel;

(II) ceramic cladding materials;

(III) fuels containing silicon carbide;

(IV) high-assay, low-enriched uranium fuels;

(V) molten-salt based liquid fuels;

(VI) fuels derived from spent nuclear fuel or depleted uranium; and

(VII) other related fuel concepts, as determined by the Commission;

(ii) activities planned or undertaken under the memorandum of understanding described in paragraph (2);

(iii) an accounting of the areas of research needed with respect to advanced nuclear fuel; and

(iv) any other challenges or considerations identified by the Commission.

(B) CONSULTATION.—In developing the report under subparagraph (A), the Commission shall seek input from—

(i) the Secretary of Energy;

(ii) National Laboratories;

(iii) the nuclear energy industry;

(iv) technology developers;

(v) nongovernmental organizations; and

(vi) other public stakeholders.

(v) COMMISSION WORKFORCE.—

(1) DEFINITION OF CHAIRMAN.—In this subsection, the term ''Chairman'' means the Chairman of the Commission.

(2) HIRING BONUS AND APPOINTMENT AUTHORITY.—

(A) IN GENERAL.—Notwithstanding section 161 d. of the Atomic Energy Act of 1954 (42 U.S.C. 2201(d)), any provision of Reorganization Plan No. 1 of 1980 (94 Stat. 3585; 5 U.S.C. app.), and any provision of title 5, United States Code, governing appointments and General Schedule classification and pay rates, the Chairman may, subject to the limitations described in subparagraph (C), and without regard to the civil service laws—

(i) establish the positions described in subparagraph (B); and

(ii) appoint persons to the positions established under clause (i).

(B) POSITIONS DESCRIBED.—The positions referred to in subparagraph (A)(i) are—

(i) permanent or term-limited positions with highly specialized scientific, engineering, and technical competencies to address a critical licensing or regulatory oversight need for the Commission, including—

(I) health physicist;

(II) reactor operations engineer;

(III) human factors analyst or engineer;

(IV) risk and reliability analyst or engineer;

(V) licensing project manager;

(VI) reactor engineer for severe accidents;

(VII) geotechnical engineer;

(VIII) structural engineer;

(IX) reactor systems engineer;

(X) reactor engineer;

(XI) radiation scientist;

(XII) seismic engineer; and

(XIII) electronics engineer; or

(ii) permanent or term-limited positions to be filled by exceptionally well-qualified individuals that the Chairman, subject to paragraph (5), determines are necessary to fulfill the mission of the Commission.

(C) LIMITATIONS.—

(i) IN GENERAL.—Appointments under subparagraph (A)(ii) may be made to not more than—

(I)(aa) 15 permanent positions described in subparagraph (B)(i) during fiscal year 2024; and

(bb) 10 permanent positions described in subparagraph (B)(i) during each fiscal year thereafter;

(II)(aa) 15 term-limited positions described in subparagraph (B)(i) during fiscal year 2024; and

(bb) 10 term-limited positions described in subparagraph (B)(i) during each fiscal year thereafter;

(III)(aa) 15 permanent positions described in subparagraph (B)(ii) during fiscal year 2024; and

(bb) 10 permanent positions described in subparagraph (B)(ii) during each fiscal year thereafter; and

(IV)(aa) 15 term-limited positions described in subparagraph (B)(ii) during fiscal year 2024; and

(bb) 10 term-limited positions described in subparagraph (B)(ii) during each fiscal year thereafter.

(ii) TERM OF TERM-LIMITED APPOINTMENT.—If a person is appointed to a term-limited position described in clause (i) or (ii) of subparagraph (B), the term of that appointment shall not exceed 4 years.

(iii) STAFF POSITIONS.—Subject to paragraph (5), appointments made to positions established under this paragraph shall be to a range of staff positions that are of entry, mid, and senior levels, to the extent practicable.

(D) HIRING BONUS.—The Commission may pay a person appointed under subparagraph (A) a 1-time hiring bonus in an amount not to exceed the least of—

(i) $25,000;

(ii) the amount equal to 15 percent of the annual rate of basic pay of the employee; and

(iii) the amount of the limitation that is applicable for a calendar year under section 5307(a)(1) of title 5, United States Code.

(3) COMPENSATION AND APPOINTMENT AUTHORITY.—

(A) IN GENERAL.—Notwithstanding section 161 d. of the Atomic Energy Act of 1954 (42 U.S.C. 2201(d)), any provision of Reorganization Plan No. 1 of 1980 (94 Stat. 3585; 5 U.S.C. app.), and chapter 51, and subchapter III of chapter 53, of title 5, United States Code, the Chairman, subject to the limitations described in subparagraph (C) and without regard to the civil service laws, may—

(i) establish and fix the rates of basic pay for the positions described in subparagraph (B); and

(ii) appoint persons to the positions established under clause (i).

(B) POSITIONS DESCRIBED.—The positions referred to in subparagraph (A)(i) are—

(i) positions with highly specialized scientific, engineering, and technical competencies to address a critical need for the Commission, including—

(I) health physicist;

(II) reactor operations engineer;

(III) human factors analyst or engineer;

(IV) risk and reliability analyst or engineer;

(V) licensing project manager;

(VI) reactor engineer for severe accidents;

(VII) geotechnical engineer;

(VIII) structural engineer;

(IX) reactor systems engineer;

(X) reactor engineer;

(XI) radiation scientist;

(XII) seismic engineer; and

(XIII) electronics engineer; or

(ii) positions to be filled by exceptionally well-qualified persons that the Chairman, subject to paragraph (5), determines are necessary to fulfill the mission of the Commission.

(C) LIMITATIONS.—

(i) IN GENERAL.—The annual rate of basic pay for a position described in subparagraph (B) may not exceed the per annum rate of salary payable for level III of the Executive Schedule under section 5314 of title 5, United States Code.

(ii) NUMBER OF POSITIONS.—Appointments under subparagraph (A)(ii) may be made to not more than—

(I) 10 positions described in subparagraph (B)(i) per fiscal year, not to exceed a total of 50 positions; and

(II) 10 positions described in subparagraph (B)(ii) per fiscal year, not to exceed a total of 50 positions.

(D) PERFORMANCE BONUS.—

(i) IN GENERAL.—Subject to clauses (ii) and (iii), an employee may be paid a 1-time performance bonus in an amount not to exceed the least of—

(I) $25,000;

(II) the amount equal to 15 percent of the annual rate of basic pay of the person; and

(III) the amount of the limitation that is applicable for a calendar year under section 5307(a)(1) of title 5, United States Code.

(ii) PERFORMANCE.—Any 1-time performance bonus under clause (i) shall be made to a person who demonstrated exceptional performance in the applicable fiscal year, including—

(I) leading a project team in a timely, efficient, and predictable licensing review to enable the safe use of nuclear technology;

(II) making significant contributions to a timely, efficient, and predictable licensing review to enable the safe use of nuclear technology;

(III) the resolution of novel or first-of-a-kind regulatory issues;

(IV) developing or implementing licensing or regulatory oversight processes to improve the effectiveness of the Commission; and

(V) other performance, as determined by the Chairman, subject to paragraph (5).

(iii) LIMITATIONS.—The Commission may pay a 1-time performance bonus under clause (i) for not more than 15 persons per fiscal year, and a person who receives a 1-time performance bonus under that clause may not receive another 1-time performance bonus under that clause for a period of 5 years thereafter.

(4) ANNUAL SOLICITATION FOR NUCLEAR REGULATOR APPRENTICESHIP NETWORK APPLICATIONS.—The Chairman, on an annual basis, shall solicit applications for the Nuclear Regulator Apprenticeship Network.

(5) APPLICATION OF MERIT SYSTEM PRINCIPLES.—To the maximum extent practicable, appointments under paragraphs (2)(A) and (3)(A) and any 1-time performance bonus under paragraph (3)(D) shall be made in accordance with the merit system principles set forth in section 2301 of title 5, United States Code.

(6) DELEGATION.—Pursuant to Reorganization Plan No. 1 of 1980 (94 Stat. 3585; 5 U.S.C. app.), the Chairman shall delegate, subject to the direction and supervision of the Chairman, the authority provided by paragraphs (2), (3), and (4) to the Executive Director for Operations of the Commission.

(7) ANNUAL REPORT.—The Commission shall include in the annual budget justification of the Commission—

(A) information that describes—

(i) the total number of and the positions of the persons appointed under the authority provided by paragraph (2);

(ii) the total number of and the positions of the persons paid at the rate determined under the authority provided by paragraph (3)(A);

(iii) the total number of and the positions of the persons paid a 1-time performance bonus under the authority provided by paragraph (3)(D);

(iv) how the authority provided by paragraphs (2) and (3) is being used, and has been used during the previous fiscal year, to address the hiring and retention needs of the Commission with respect to the positions described in those subsections to which that authority is applicable;

(v) if the authority provided by paragraphs (2) and (3) is not being used, or has not been used, the reasons, including a justification, for not using that authority; and

(vi) the attrition levels with respect to the term-limited appointments made under paragraph (2), including, with respect to persons leaving a position before completion of the applicable term of service, the average length of service as a percentage of the term of service;

(B) an assessment of—

(i) the current critical workforce needs of the Commission, including any critical workforce needs that the Commission anticipates in the subsequent 5 fiscal years; and

(ii) further skillsets that are or will be needed for the Commission to fulfill the licensing and oversight responsibilities of the Commission; and

(C) the plans of the Commission to assess, develop, and implement updated staff performance standards, training procedures, and schedules.

(8) REPORT ON ATTRITION AND EFFECTIVENESS.—Not later than September 30, 2032, the Commission shall submit to the Committees on Appropriations and Environment and Public Works of the Senate and the Committees on Appropriations and Energy and Commerce of the House of Representatives a report that—

(A) describes the attrition levels with respect to the term-limited appointments made under paragraph (2), including, with respect to persons leaving a position before completion of the applicable term of service, the average length of service as a percentage of the term of service;

(B) provides the views of the Commission on the effectiveness of the authorities provided by paragraphs (2) and (3) in helping the Commission fulfill the mission of the Commission; and

(C) makes recommendations with respect to whether the authorities provided by paragraphs (2) and (3) should be continued, modified, or discontinued.

(w) COMMISSION CORPORATE SUPPORT FUNDING.—

(1) REPORT.—Not later than 3 years after the date of enactment of this Act, the Commission shall submit to the appropriate committees of Congress and make publicly available a report that describes—

(A) the progress on the implementation of section 102(a)(3) of the Nuclear Energy Innovation and Modernization Act (42 U.S.C. 2215(a)(3)); and

(B) whether the Commission is meeting and is expected to meet the total budget authority caps required for corporate support under that section.

(2) LIMITATION ON CORPORATE SUPPORT COSTS.—Section 102(a)(3) of the Nuclear Energy Innovation and Modernization Act (42 U.S.C. 2215(a)(3)) is amended by striking subparagraphs (B) and (C) and inserting the following:

''(B) 30 percent for fiscal year 2024 and each fiscal year thereafter.''.

(3) CORPORATE SUPPORT COSTS CLARIFICATION.—Paragraph (9) of section 3 of the Nuclear Energy Innovation and Modernization Act (42 U.S.C. 2215 note; Public Law 115–439) (as redesignated by subsection (g)(1)(A)) is amended—

(A) by striking ''The term'' and inserting the following:

''(A) IN GENERAL.—The term''; and

(B) by adding at the end the following:

''(B) EXCLUSIONS.—The term 'corporate support costs' does not include—

''(i) costs for rent and utilities relating to any and all space in the Three White Flint North building that is not occupied by the Commission; or

''(ii) costs for salaries, travel, and other support for the Office of the Commission.''.

(x) PERFORMANCE AND REPORTING UPDATE.—Section 102(c) of the Nuclear Energy Innovation and Modernization Act (42 U.S.C. 2215(c)) is amended—

(1) in paragraph (3)—

(A) in the paragraph heading, by striking ''180'' and inserting ''90''; and

(B) by striking ''180'' and inserting ''90''; and

(2) by adding at the end the following:

''(4) PERIODIC UPDATES TO METRICS AND SCHEDULES.—

''(A) REVIEW AND ASSESSMENT.—Not less frequently than once every 3 years, the Commission shall review and assess, based on the licensing and regulatory activities of the Commission, the performance metrics and milestone schedules established under paragraph (1).

''(B) REVISIONS.—After each review and assessment under subparagraph (A), the Commission shall revise and improve, as appropriate, the performance metrics and milestone schedules described in that subparagraph to provide the most efficient metrics and schedules reasonably achievable.''.

(y) NUCLEAR CLOSURE COMMUNITIES.—

(1) DEFINITIONS.—In this subsection:

(A) COMMUNITY ADVISORY BOARD.—The term ''community advisory board'' means a community committee or other advisory organization that aims to foster communication and information exchange between a licensee planning for and involved in decommissioning activities and members of the community that decommissioning activities may affect.

(B) DECOMMISSION.—The term ''decommission'' has the meaning given the term in section 50.2 of title 10, Code of Federal Regulations (or successor regulations).

(C) ELIGIBLE RECIPIENT.—The term ''eligible recipient'' has the meaning given the term in section 3 of the Public Works and Economic Development Act of 1965 (42 U.S.C. 3122).

(D) LICENSEE.—The term ''licensee'' has the meaning given the term in section 50.2 of title 10, Code of Federal Regulations (or successor regulations).

(E) NUCLEAR CLOSURE COMMUNITY.—The term ''nuclear closure community'' means a unit of local government, including a county, city, town, village, school district, or special district, that has been impacted, or reasonably demonstrates to the satisfaction of the Secretary that it will be impacted, by a nuclear power plant licensed by the Commission that—

(i) is not co-located with an operating nuclear power plant;

(ii) is at a site with spent nuclear fuel; and

(iii) as of the date of enactment of this Act—

(I) has ceased operations; or

(II) has provided a written notification to the Commission that it will cease operations.

(F) SECRETARY.—The term ''Secretary'' means the Secretary of Commerce, acting through the Assistant Secretary of Commerce for Economic Development.

(2) ESTABLISHMENT.—Not later than 180 days after the date of enactment of this Act, the Secretary shall establish a grant program to provide grants to eligible recipients—

(A) to assist with economic development in nuclear closure communities; and

(B) to fund community advisory boards in nuclear closure communities.

(3) REQUIREMENT.—In carrying out this subsection, to the maximum extent practicable, the Secretary shall implement the recommendations described in the report submitted to Congress under section 108 of the Nuclear Energy Innovation and Modernization Act (Public Law 115–439; 132 Stat. 5577) entitled ''Best Practices for Establishment and Operation of Local Community Advisory Boards Associated with Decommissioning Activities at Nuclear Power Plants''.

(4) DISTRIBUTION OF FUNDS.—The Secretary shall establish a formula to ensure, to the maximum extent practicable, geographic diversity among grant recipients under this subsection.

(5) AUTHORIZATION OF APPROPRIATIONS.—

(A) IN GENERAL.—There are authorized to be appropriated to the Secretary—

(i) to carry out paragraph (2)(A), $35,000,000 for each of fiscal years 2023 through 2028; and

(ii) to carry out paragraph (2)(B), $5,000,000 for each of fiscal years 2023 through 2025.

(B) AVAILABILITY.—Amounts made available under this subsection shall remain available for a period of 5 years beginning on the date on which the amounts are made available.

(C) NO OFFSET.—None of the funds made available under this subsection may be used to offset the funding for any other Federal program.

(z) TECHNICAL CORRECTION.—Section 104 c. of the Atomic Energy Act of 1954 (42 U.S.C. 2134(c)) is amended—

(1) by striking the third sentence and inserting the following:

''(3) LIMITATION ON UTILIZATION FACILITIES.—The Commission may issue a license under this section for a utilization facility useful in the conduct of research and development activities of the types specified in section 31 if—

''(A) not more than 75 percent of the annual costs to the licensee of owning and operating the facility are devoted to the sale, other than for research and development or education and training, of—

''(i) nonenergy services;

''(ii) energy; or

''(iii) a combination of nonenergy services and energy; and

''(B) not more than 50 percent of the annual costs to the licensee of owning and operating the facility are devoted to the sale of energy.'';

(2) in the second sentence, by striking ''The Commission'' and inserting the following:

''(2) REGULATION.—The Commission''; and

(3) by striking ''c. The Commission'' and inserting the following:

''c. RESEARCH AND DEVELOPMENT ACTIVITIES.—

''(1) IN GENERAL.—Subject to paragraphs (2) and (3), the Commission''.

(aa) REPORT ON ENGAGEMENT WITH THE GOVERNMENT OF CANADA WITH RESPECT TO NUCLEAR WASTE ISSUES IN THE GREAT LAKES BASIN.—Not later than 1 year after the date of enactment of this Act, the Commission shall submit to Congress a report describing any engagement between the Commission and the Government of Canada with respect

to nuclear waste issues in the Great Lakes Basin.

SA 797. Mr. SCHUMER (for himself, Mr. ROUNDS, Mr. RUBIO, Mrs. GILLIBRAND, Mr. YOUNG, and Mr. HEINRICH) submitted an amendment intended to be proposed by him to the bill S. 2226, to authorize appropriations for fiscal year 2024 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

TITLE __—UNIDENTIFIED ANOMALOUS PHENOMENA DISCLOSURE

SEC. ___01. SHORT TITLE.

This title may be cited as the ''Unidentified Anomalous Phenomena Disclosure Act of 2023'' or the ''UAP Disclosure Act of 2023''.

SEC. ___02. FINDINGS, DECLARATIONS, AND PURPOSES.

(a) FINDINGS AND DECLARATIONS.—Congress finds and declares the following:

(1) All Federal Government records related to unidentified anomalous phenomena should be preserved and centralized for historical and Federal Government purposes.

(2) All Federal Government records concerning unidentified anomalous phenomena should carry a presumption of immediate disclosure and all records should be eventually disclosed to enable the public to become fully informed about the history of the Federal Government's knowledge and involvement surrounding unidentified anomalous phenomena.

(3) Legislation is necessary to create an enforceable, independent, and accountable process for the public disclosure of such records.

(4) Legislation is necessary because credible evidence and testimony indicates that Federal Government unidentified anomalous phenomena records exist that have not been declassified or subject to mandatory declassification review as set forth in Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information) due in part to exemptions under the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.), as well as an over-broad interpretation of ''transclassified foreign nuclear information'', which is also exempt from mandatory declassification, thereby preventing public disclosure under existing provisions of law.

(5) Legislation is necessary because section 552 of title 5, United States Code (commonly referred to as the ''Freedom of Information Act''), as implemented by the Executive branch of the Federal Government, has proven inadequate in achieving the timely public disclosure of Government unidentified anomalous phenomena records that are subject to mandatory declassification review.

(6) Legislation is necessary to restore proper oversight over unidentified anomalous phenomena records by elected officials in both the executive and legislative branches of the Federal Government that has otherwise been lacking as of the enactment of this Act.

(7) Legislation is necessary to afford complete and timely access to all knowledge gained by the Federal Government concerning unidentified anomalous phenomena in furtherance of comprehensive open scientific and technological research and development essential to avoiding or mitigating potential technological surprise in furtherance of urgent national security concerns and the public interest.

(b) PURPOSES.—The purposes of this title are—

(1) to provide for the creation of the unidentified anomalous phenomena Records Collection at the National Archives and Records Administration; and

(2) to require the expeditious public transmission to the Archivist and public disclosure of such records.

SEC. ___03. DEFINITIONS.

In this title:

(1) ARCHIVIST.—The term ''Archivist'' means the Archivist of the United States.

(2) CLOSE OBSERVER.—The term ''close observer'' means anyone who has come into close proximity to unidentified anomalous phenomena or non-human intelligence.

(3) COLLECTION.—The term ''Collection'' means the Unidentified Anomalous Phenomena Records Collection established under section ___04.

(4) CONTROLLED DISCLOSURE CAMPAIGN PLAN.—The term ''Controlled Disclosure Campaign Plan'' means the Controlled Disclosure Campaign Plan required by section ___09(c)(3).

(5) CONTROLLING AUTHORITY.—The term ''controlling authority'' means any Federal, State, or local government department, office, agency, committee, commission, commercial company, academic institution, or private sector entity in physical possession of technologies of unknown origin or biological evidence of non-human intelligence.

(6) EXECUTIVE AGENCY.—The term ''Executive agency'' means an Executive agency, as defined in subsection 552(f) of title 5, United States Code.

(7) GOVERNMENT OFFICE.—The term ''Government office'' means any department, office, agency, committee, or commission of the Federal Government and any independent office or agency without exception that has possession or control, including via contract or other agreement, of unidentified anomalous phenomena records.

(8) IDENTIFICATION AID.—The term ''identification aid'' means the written description prepared for each record, as required in section ___04.

(9) LEADERSHIP OF CONGRESS.—The term ''leadership of Congress'' means—

(A) the majority leader of the Senate;

(B) the minority leader of the Senate;

(C) the Speaker of the House of Representatives; and

(D) the minority leader of the House of Representatives.

(10) LEGACY PROGRAM.—The term ''legacy program'' means all Federal, State, and local government, commercial industry, academic, and private sector endeavors to collect, exploit, or reverse engineer technologies of unknown origin or examine biological evidence of living or deceased non-human intelligence that pre-dates the date of the enactment of this Act.

(11) NATIONAL ARCHIVES.—The term ''National Archives'' means the National Archives and Records Administration and all components thereof, including presidential archival depositories established under section 2112 of title 44, United States Code.

(12) NON-HUMAN INTELLIGENCE.—The term ''non-human intelligence'' means any sentient intelligent non-human lifeform regardless of nature or ultimate origin that may be presumed responsible for unidentified anomalous phenomena or of which the Federal Government has become aware.

(13) ORIGINATING BODY.—The term ''originating body'' means the Executive agency, Federal Government commission, committee of Congress, or other Governmental entity that created a record or particular information within a record.

(14) PROSAIC ATTRIBUTION.—The term ''prosaic attribution'' means having a human (either foreign or domestic) origin and operating according to current, proven, and generally understood scientific and engineering principles and established laws-of-nature and not attributable to non-human intelligence.

(15) PUBLIC INTEREST.—The term ''public interest'' means the compelling interest in the prompt public disclosure of unidentified anomalous phenomena records for historical and Governmental purposes and for the purpose of fully informing the people of the United States about the history of the Federal Government's knowledge and involvement surrounding unidentified anomalous phenomena.

(16) RECORD.—The term ''record'' includes a book, paper, report, memorandum, directive, email, text, or other form of communication, or map, photograph, sound or video recording, machine-readable material, computerized, digitized, or electronic information, including intelligence, surveillance, reconnaissance, and target acquisition sensor data, regardless of the medium on which it is stored, or other documentary material, regardless of its physical form or characteristics.

(17) REVIEW BOARD.—The term ''Review Board'' means the Unidentified Anomalous Phenomena Records Review Board established by section ___07.

(18) TECHNOLOGIES OF UNKNOWN ORIGIN.—The term ''technologies of unknown origin'' means any materials or meta-materials, ejecta, crash debris, mechanisms, machinery, equipment, assemblies or sub-assemblies, engineering models or processes, damaged or intact aerospace vehicles, and damaged or intact ocean-surface and undersea craft associated with unidentified anomalous phenomena or incorporating science and technology that lacks prosaic attribution or known means of human manufacture.

(19) TEMPORARILY NON-ATTRIBUTED OBJECTS.—

(A) IN GENERAL.—The term ''temporarily non-attributed objects'' means the class of objects that temporarily resist prosaic attribution by the initial observer as a result of environmental or system limitations associated with the observation process that nevertheless ultimately have an accepted human origin or known physical cause. Although some unidentified anomalous phenomena may at first be interpreted as temporarily non-attributed objects, they are not temporarily non-attributed objects, and the two categories are mutually exclusive.

(B) INCLUSION.—The term ''temporarily non-attributed objects'' includes—

(i) natural celestial, meteorological, and undersea weather phenomena;

(ii) mundane human-made airborne objects, clutter, and marine debris;

(iii) Federal, State, and local government, commercial industry, academic, and private sector aerospace platforms;

(iv) Federal, State, and local government, commercial industry, academic, and private sector ocean-surface and undersea vehicles; and

(v) known foreign systems.

(20) THIRD AGENCY.—The term ''third agency'' means a Government agency that originated a unidentified anomalous phenomena record that is in the possession of another Government agency.

(21) UNIDENTIFIED ANOMALOUS PHENOMENA.—

(A) IN GENERAL.—The term ''unidentified anomalous phenomena'' means any object operating or judged capable of operating in outer-space, the atmosphere, ocean surfaces, or undersea lacking prosaic attribution due to performance characteristics and properties not previously known to be achievable