and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4613. Mr. SCOTT of Florida submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4614. Ms. MURKOWSKI submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4615. Mr. SANDERS submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4616. Mr. COONS submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4617. Ms. SINEMA submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4618. Mr. COONET submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4619. Mr. SULLIVAN (for himself and Mr. WHITEHOUSE) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4620. Mr. COTTON (for himself, Mr. MANCHIN, Mr. TUBERVILLE, and Mr. KELLY) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4621. Mr. BROWN (for himself and Mr. WARNER) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4622. Mrs. BLACKBURN submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4623. Mr. MARKEY submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4624. Mr. BARRASSO submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4625. Mr. BARRASSO submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4626. Mr. TOOMEY submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4627. Mr. ROUNDS (for himself and Mr. VAN HOLLEN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4628. Mr. LEE submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4629. Mr. MENENDEZ submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4630. Mr. MACHIN (for himself, Mrs. CAPRITO, Mr. HUNTSMAN, Mr. COTTON, Mrs. BLACKBURN, and Mr. TESSER) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4631. Mr. SCOTT of Florida submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4632. Mr. WARNER submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SEC. 1285. RULE OF CONSTRUCTION REGARDING THE CONSTITUTIONAL POWERS OF THE PRESIDENT AS COMMANDER-IN-CHIEF.

Nothing in this Act shall be construed to infringe upon the constitutional powers of the President as Commander-in-Chief under Article II of the Constitution of the United States.

SA 4784. Mr. KING (for himself, Mr. ROUNDS, Mr. SASSE, Ms. ROSEN, Ms. HARRASS, and Mr. OSSTOFF) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 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:

DIVISION E—DEFENSE OF UNITED STATES INFRASTRUCTURE

SEC. 5001. SHORT TITLE.

This division may be cited as the ‘‘Defense of United States Infrastructure Act of 2021’’.

SEC. 5002. DEFINITIONS.

In this division:

(1) CRITICAL INFRASTRUCTURE.—The term ‘‘critical infrastructure’’ has the meaning given such term in section 101(e) of the Critical Infrastructure Protection Act of 2001 (42 U.S.C. 5190e(c)).

(2) CYBERSECURITY RISK.—The term ‘‘cybersecurity risk’’ has the meaning given such term in section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659).

(3) DEPARTMENT.—The term ‘‘Department’’ means the Department of Homeland Security.

(4) SECRETARY.—The term ‘‘Secretary’’ means the Secretary of Homeland Security.

TITLE LI—INVESTING IN CYBER RESILIENCE AND CRITICAL INFRASTRUCTURE

SEC. 5101. NATIONAL RISK MANAGEMENT CYCLE.

(a) AMENDMENTS.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(1) in section 2212(c) (6 U.S.C. 651e(c))—

(A) in paragraph (11), by striking ‘‘and’’ at the end;

(B) in the first paragraph designated as paragraph (12), by striking the following—

‘‘(i) by redesigning section 2217 (6 U.S.C. 665) as section 2220;’’—

(2) by redesigning subsections (a), (b), and (c) of section 2218;

(3) by redesigning sections 2216 (6 U.S.C. 665e) as section 2219;

(4) by redesigning the fourth and fifth sections (relating to Sector Risk Management Agencies) (6 U.S.C. 665f) as section 2218;

(5) by redesigning the third and fourth sections (relating to the Cybersecurity State Coordinator) (6 U.S.C. 665c) as section 2217;

(6) by redesigning the second and third sections (relating to the Joint Cyber Planning Office) (6 U.S.C. 665b) as section 2216; and

(7) by adding at the end the following—

‘‘SEC. 2220A. NATIONAL RISK MANAGEMENT CYCLE.

(a) NATIONAL CRITICAL FUNCTIONS DEFINED.—In this section, the term ‘‘national critical functions’’ means the functions of

The President is authorized to use the Armed Forces of the United States as the President determines to be necessary and appropriate in order to defend the national security of the United States against the threat posed by the Islamic State of Iraq and Syria (ISIS) and associated forces in Iraq.

This division may be cited as the ‘‘Defense of United States Infrastructure Act of 2021’’.

This division may be cited as the ‘‘Defense of United States Infrastructure Act of 2021’’.

This division may be cited as the ‘‘Defense of United States Infrastructure Act of 2021’’.

This division may be cited as the ‘‘Defense of United States Infrastructure Act of 2021’’.
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, assess, and prioritize risks to critical infrastructure, considering the physical and technological vulnerabilities, the associated likelihoods, vulnerabilities, and consequences, and the resources necessary to mitigate such risks.

"(B) CONSULTATION.—In establishing the process required under subparagraph (A), the Secretary shall consult with, and request and collect information from, Sector Risk Management Agencies, critical infrastructure owners and operators, the Assistant to the President for National Security Affairs, the Assistant to the President for Homeland Security, and the National Cyber Director.

"(c) 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.

"(d) 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).

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

"(2) 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 (Public Law 116–233).

"(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 of the House, and the minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, 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) identify, assess, and prioritize risks to critical infrastructure that may compromise or disrupt national critical functions impacting national security, economic security, or public health and safety;

"(ii) identify and outline current and proposed actions, programs, and efforts to be taken to address the risks identified;

"(iii) identify and outline current and proposed actions, programs, and efforts to be taken to address the risks identified.

"(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 a strategy under this section, and every year thereafter, the Secretary, in coordination with Sector Risk Management Agencies, shall brief the appropriate committees of Congress on—

"(A) the national risk management cycle activities undertaken pursuant to the strategy; 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.

"(C) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) TABLE OF CONTENTS.—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 the item relating to the sentence item through the item relating to section 2117 and inserting the following:

Sec. 2114. National Asset Database.
Sec. 2115. Duties relating to .gov internet domain.
Sec. 2116. Joint Cyber Planning Office.
Sec. 2117. Cybersecurity State Coordinator.
Sec. 2119. Cybersecurity Advisory Committee.
Sec. 2220. Cybersecurity education and training programs.
Sec. 2220A. National risk management cycle.

(2) ADDITIONAL TECHNICAL AMENDMENT.—

(A) AMENDMENT.—Section 904(b)(1) of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260) is amended, in the matter preceding subparagraph (A), by striking "Homeland Security Act" and inserting "Homeland Security Act of 2002".

(B) EFFECTIVE DATE.—The amendment made by subparagraph (A) shall take effect as if enacted as part of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260).

TITLE XII—IMPROVING THE ABILITY OF THE FEDERAL GOVERNMENT TO ASSIST IN ENHANCING CRITICAL INFRASTRUCTURE CYBER RESILIENCE

SEC. 2501. INSTITUTE A 5-YEAR TERM FOR THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

(a) In General.—Subsection (b)(1) of section 2202 of the Homeland Security Act of 2002 (6 U.S.C. 652), is amended by inserting "The term of office of an individual serving as Director shall be 5 years." after "who shall report to the Secretary.".

(b) Transition Rules.—The amendment made by subsection (a) shall take effect on the first appointment of an individual to the position of Director of the Cybersecurity and Infrastructure Security Agency, by and with the advice and consent of the Senate, that is made on or after the date of enactment of this Act.

SEC. 2502. CYBER THREAT INFORMATION COLLABORATION ENVIRONMENT.

(a) Definitions.—In this section:

"(1) CRITICAL INFRASTRUCTURE INFORMATION.—The term "critical infrastructure information" has the meaning given such term in section 2222 of the Homeland Security Act of 2002 (6 U.S.C. 671).

"(2) CYBER THREAT INDICATOR.—The term "cyber threat indicator" has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

"(3) CYBERSECURITY THREAT.—The term "cybersecurity threat" has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

"(4) ENVIRONMENT.—The term "environment" means the information collaboration environment established under subsection (b).

"(5) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term "information sharing and analysis organization" has the meaning given such term in section 2222 of the Homeland Security Act of 2002 (6 U.S.C. 1501).

(b) Program.—The Secretary, in consultation with the Secretary of Defense, the Director of National Intelligence, and the Attorney General, shall carry out a program under which the Secretary shall develop an information collaboration environment consisting of a digital environment containing technical tools for information analytics and a portal through which relevant parties may submit and automatically receive information inputs and access the environment in order to enable interoperable data flows that enable Federal and non-Federal entities to identify, mitigate, and prevent malicious cyber activity to—

"(1) provide limited access to appropriate and operationally relevant data from unclassified and non-classified intelligence about cyber security risks and cybersecurity threats, as well as malware forensics and data from network sensor programs,

"(2) enable cross-correlation of data on cyber security risks and cybersecurity threats at the speed and scale necessary for rapid detection and identification of threats,

"(3) facilitate a comprehensive understanding of cybersecurity risks and cybersecurity threats; and

"(4) facilitate collaborative analysis between the Federal Government and public and private sector critical infrastructure entities and information and analysis organizations.

(c) IMPLEMENTATION OF INFORMATION COLLABORATION ENVIRONMENT.—

"(1) EVALUATION.—Not later than 180 days after the date of enactment of this Act, the Secretary, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, and in coordination with the Secretary of Defense, the Director of National Intelligence, and the Attorney General, shall—

"(A) identify, inventory, and evaluate existing Federal sources of classified and unclassified information on cybersecurity threats;

"(B) evaluate current programs, applications, or platforms intended to detect, identify, analyze, and monitor cyber threat capabilities, needs, and gaps;

"(C) consult with public and private sector critical infrastructure entities to identify public and private critical infrastructure cyber threat capabilities, needs, and gaps; and

"(D) identify existing tools, capabilities, and systems that may be adapted to achieve the purposes of the environment in order to maximize return on investment and minimize cost.

"(2) IMPLEMENTATION.—Not later than 1 year after completing the evaluation required under paragraph (1), the Secretary, acting through the Director of the Cybersecurity and Infrastructure Security Agency, and in consultation with the Secretary of Defense, the Director of National Intelligence, and...
the Attorney General, shall begin implementation of the environment to develop and run analytic tools referred to in subsection (b) on specific threats to the purposes of detec-
tifying, mitigating, and preventing malicious cyber activity that is a threat to public and private critical infrastructure.

(b) The environment and the use of analytic tools referred to in subsection (b) shall—

(1) operate in a manner consistent with rele-
vant laws and regulations, and civil liberties and
privacy protections and standards, including such poli-
ties and protections established pursuant to section 1016 of the Intelligence Reform and

(i) account for appropriate data interopera-
tility requirements;

(ii) enable integration of current appli-
cations, platforms, data, and information, in-
cluding classified information, in a manner that
supports the voluntary integration of unclassified and classified information on cybersecurity risks and cybersecurity threats;

(iv) incorporate tools to manage access to
classified and unclassified data, as appro-
prate;

(v) ensure accessibility by entities the Sec-
retary, in consultation with the Secretary of
Defense, the Director of National Intelli-
gen, and the Attorney General, deter-
nates appropriate;

(vi) allow for access by critical infrastruc-
ture stakeholders and other private sector partners, at the discretion of the Secretary,

(2) DATA STREAMS.—The Secretary, in co-
ordination with the heads of appropriate de-
partments and agencies, shall identify, des-
ignate, and periodically update programs that shall participate in or be interoperable
with the environment, in a manner con-
sistent with data security standards under
Federal law, which may include—

(A) network-monitoring and intrusion de-
tection programs;

(B) threat indicator sharing pro-
gress;

(C) certain government-sponsored network

and network-monitoring programs;

(D) incident response and cybersecurity
technical assistance programs; or

(E) malware forensics and reverse-engineering programs.

(3) DATA GOVERNANCE.—The Secretary, in co-
ordination with the Secretary of Defense, the Director of National Intelligence,
and the Attorney General, shall establish proce-
dures and data governance structures, as
necessary, to protect data shared in the envi-
ronment, in a manner consistent with Federal regulations and statutes, and respect existing consent
agreements with private sector critical infra-
structure entities that apply to critical infra-
structure programs.

(4) RULE OF CONSTRUCTION.—Nothing in this
subsection shall change existing ownership or protection of, or policies and processes for
access to, agency data.

(e) NATIONAL SECURITY SYSTEMS.—Nothing in
this section shall apply to national secu-

ity systems, as defined in section 3522 of title 44, United States Code, or to cyberse-
curity threat intelligence related to such sys-
tems, without the consent of the relevant
principals in the national security community, as defined in section 3 of the National Security

(f) PROTECTION OF INTELLIGENCE SOURCES
AND METHODS.—The Director of National In-

telligence shall ensure that any information
sharing conducted under this section shall

(g) DURATION.—The program under this
section shall continue until the date that is 5 years after the date of enactment of this Act.

TITLE LI—ENABLING THE NATIONAL CYBER DIRECTOR

SEC. 5401. ESTABLISHMENT OF HIRING AUTHORITY

(a) DEFINITIONS.—In this section:

(1) DIRECTOR.—The term ‘‘Director’’ means

(2) EXCEPTED SERVICE.—The term ‘‘ex-
cepted service’’ has the meaning given such
term in section 2101 of title 5, United States
Code.

(3) OFFICE.—The term ‘‘Office’’ means the

(b) DEFINITIONS.—In this section:

(1) DIRECTOR.—The term ‘‘Director’’ means

(2) EXCEPTED SERVICE.—The term ‘‘ex-
cepted service’’ has the meaning given such
term in section 2101 of title 5, United States
Code.

(3) OFFICE.—The term ‘‘Office’’ means the

(c) DEFINITIONS.—In this section:

(1) DIRECTOR.—The term ‘‘Director’’ means

(2) OFFICE.—The term ‘‘Office’’ means the

TITLES VI—FEDERAL AHSTRUSTS
a report on the status and progress of implementation of the grant program under this section, including on the number and nature of institutions participating, the number and nature of institutions receiving grants, the level of funding provided to grant recipients, the types of activities being funded by the grants program, and plans for future implementation and development;

(2) 5 years after the effective date of this section, as provided in subsection (b), the Director shall prepare and submit to Congress a report on the status of cybersecurity education programming and capacity-building at institutions receiving grants under this section, including data and scope of these programs, associated facilities, or in accreditation status, and on the educational and employment outcomes of cybersecurity programs that have received support under this section.

(g) PERFORMANCE METRICS.—The Director shall establish performance metrics for grants awarded under this section.

(h) EFFECTIVE DATE.—This section shall take effect 1 year after the date of enactment of this Act.

SA 4786. Mr. MENENDEZ (for himself, Mr. SCHUMER, Mr. BOOKER, Ms. GILLIBRAND, Mr. BLUMENTHAL, and Mr. MURPHY) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 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:

SEC. APPROPRIATIONS FOR CATCH-UP PAYMENTS.

Section 404(d)(4)(C) of the Justice for United States Victims of State Sponsored Terrorism Act (42 U.S.C. 2014(d)(4)(C)) is amended by adding the following:

"(IV) FUNDING.—

"(bb) APPROPRIATIONS.—

"(I) IN GENERAL.—There are authorized to be appropriated for each fiscal year to the Fund such sums as may be necessary to carry out this paragraph, to remain available until expended.

"(II) EMERGENCY DESIGNATION.—The amounts provided under this subclause are designated as an emergency requirement pursuant to section 252(b)(6) of the Pay-As-You-Go Act of 2010 (2 U.S.C. 933(g)).

"(cc) DESIGNATION IN THE HOUSE AND SENATE.—This subclause is designated by the Director first awards a grant under subsection (a) shall submit an application to the Director at such time, in such manner, and with such information as the Director may reasonably require, including a statement of how the institution will use the funds awarded that the funds are intended to expand individual security education opportunities at the eligible institution.

(e) ACTIVITIES.—An eligible institution that receives a grant under this section may use the funds awarded through such grant for increasing research, education, technical, partnership, and innovation capacity, including for:

(1) building and upgrading institutional capacity to better support new or existing cybersecurity partnerships, including cybersecurity partnerships with public and private entities;

(2) building and upgrading institutional capacity to better support new or existing cybersecurity partnerships, including cybersecurity partnerships with public and private entities;

(3) outreach to students to increase awareness of new or existing cybersecurity programs, including cybersecurity partnerships with public and private entities;

(4) REPORTING REQUIREMENTS.—Not later than—

(1) 1 year after the effective date of this section, as provided in subsection (b), and annually thereafter until the Director submits the report under paragraph (2), the Director shall prepare and submit to Congress
health, the Patient Protection and Affordable Care Act (Public Law 111–148) requires all non-grandfathered individual and group health plans to cover without cost-sharing preventive care, including evidence-based preventive services for women supported by the Health Resources and Services Administration of the Department of Health and Human Services. These evidence-based preventive services include the full range of female-controlled contraceptive methods, elective family planning practices, and sterilization procedures approved by the Food and Drug Administration. The Health Resources and Services Administration has affirmed that contraceptive care includes contraceptive counseling, initiation of contraceptive use, and follow-up care (such as management, evaluation, and changes to and removal or discontinuation of the contraceptive method).

(9) The Defense Advisory Committee on Women in the Services has recommended that all the Armed Forces, to the extent that they have not already, implement initiatives that inform members of the Armed Forces of the importance of family planning, educate them on methods of contraception, and make various contraceptives available, based on the finding that family planning can increase the overall readiness and quality of life of all members of the Armed Forces.

(10) The military departments received more than 7,300 reports of sexual assaults involving members of the Armed Forces as victims during fiscal year 2019. Through regulations, the Department of Defense already supports a policy ensuring that the Secretary of Defense provides a service to all persons who are victims of sexual assault, and the Secretary of Defense may provide care to members of the Armed Forces who are sexually assaulted in a facility that is provided to members of the Armed Forces as follows:

SEC. 763. CONSIDERATION OF PRIVACY AND SECURITY UNDER THE TRICARE PROGRAM.

(a) PHARMACY BENEFITS PROGRAM.—Section 1074a(a)(6) of title 10, United States Code, is amended by adding at the end the following new section:

"(4) Notwithstanding any other provision of this section, cost-sharing requirements may not be imposed and cost-sharing amounts may not be collected with respect to any beneficiary enrolled in TRICARE Prime for a service described in paragraph (2) that is provided under TRICARE Prime.

(2) A service described in this paragraph is any method of contraception approved by the Food and Drug Administration, any contraceptive device (whether inserted, removed, and follow up), any sterilization procedure, or any patient education or counseling service provided in connection with any such method, care, or procedure.

(b) TRICARE SELECT.—Section 1075 of such title is amended by adding at the end the following new paragraph:

"1075p. Provision of pregnancy prevention assistance at military medical treatment facilities

(a) INFORMATION AND ASSISTANCE.—The Secretary of Defense shall promptly furnish to sexual assault survivors at each military medical treatment facility the following:

(1) Comprehensive, medically and factually accurate, and unbiased written and oral information about all methods of emergency contraception approved by the Food and Drug Administration.

(2) Upon request by the sexual assault survivor, emergency contraception or, if applicable, a prescription for emergency contraception.

(3) Notification of the right of the sexual assault survivor to confidentiality with respect to the information and care and services furnished under this section.

(b) INFORMATION.—The Secretary shall ensure that information provided pursuant to subsection (a) is provided in language that—

(1) is clear and concise;

(2) is readily comprehensible; and

(3) meets such conditions (including conditions regarding the provision of information in languages other than English) as the Secretary may prescribe in regulations to carry out this section.

(c) DEFINITIONS.—In this section:

(1) The term "sexual assault survivor" means any individuals at a military medical treatment facility—

(A) who are B described in this paragraph as a service described in paragraph (2) that is provided by a network provider; or

(B) who are provided to members of the Armed Forces by a network provider.

(b) TRICARE SELECT.—The table of sections of chapters 77 and 96 of title 10, United States Code, is amended by adding after the item relating to section 1074a the following new item:

"1074p. Provision of pregnancy prevention assistance at military medical treatment facilities.

(c) ELEMENTS.—The uniform standard curriculum for education programs under subsection (a) and (b) of this section should be evidence-informed and include the use of the latest technology available to efficiently and effectively deliver information to the members of the Armed Forces.

(d) INFORMATION.—The uniform standard curriculum and programs under subsections (a) and (b) of this section shall include the following:

(1) Information on—

(A) the importance of providing comprehensive family planning for members of the Armed Forces, including commanding officers; and

(B) the positive impact family planning can have on the health and readiness of the Armed Forces.

(2) Information on—

(A) the full range of methods of contraception approved by the Food and Drug Administration; and

(B) where members of the Armed Forces can access their chosen method of contraception.

(3) Information on all applicable laws and policies so that members of the Armed Forces are informed of their rights and obligations.

(7) Information on the rights of patients to confidentiality.

(8) Information on the unique circumstances encountered by members of the Armed Forces and the effects of such circumstances on the use of contraception.

SA 4788. Mr. LEY submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4330, to authorize appropriations for fiscal year 2022 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:

On page 621, strike lines 11 through 24 and insert the following:

(cross-strait relations;

(7) reinforcing the status of the Republic of Singapore as a Major Non-Nato Partner of the United States and continuing to strengthen defense and security cooperation between the military forces of the Republic of Singapore and the United States, including through participation in combined exercises and training, including the use of the Foreign Military Sales Training Center at Joint Base Pearl Harbor-Hickam, Hawaii, and continuing to support the Republic of Singapore as an important ally in the Indo-Pacific region.

SA 4789. Mr. LEY submitted an amendment intended to be proposed to
amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 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:

On page 578, strike lines 14 through 19 and insert the following:

"(1) by striking ‘‘fiscal year 2021’’ and inserting ‘‘fiscal year 2022’’; and

(2) by striking ‘‘fiscal year 2021’’ and inserting ‘‘fiscal year 2022’’ specified in the funding table of Division D of this Act’."

SA 4790. Mr. LEE submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 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:

Strike section 1061.

SA 4791. Mr. MORAN (for himself and Ms. ROSEN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 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 of subtitle C of title VII, add the following:

SEC. 744. GRANT PROGRAM FOR INCREASED COVERAGE OF POST-TRAUMATIC STRESS DISORDER RESEARCH BETWEEN UNITED STATES AND ISRAEL.

(a) FINDING.—Congress makes the following findings:

(1) The Department of Veterans Affairs reports that between 11 and 20 percent of veterans who served in Operation Iraqi Freedom and Operation Enduring Freedom have post-traumatic stress disorder (in this paragraph referred to as ‘‘PTSD’’) in a given year. In addition, that figure amounts to about 12 percent of Gulf War veterans and up to 30 percent of Vietnam veterans.

(2) The Department of Veterans Affairs reports that among women veterans of the conflicts in Iraq and Afghanistan, almost 20 percent have been diagnosed with PTSD.

(3) It is thought that 70 percent of individuals in the United States have experienced at least one traumatic event in their lifetime, and approximately 20 percent of those individuals have struggled or continue to struggle with symptoms of PTSD.

(4) Studies show that PTSD has links to homelessness and substance abuse in the United States. Department of Veterans Affairs estimates that approximately 11 percent of the homeless population are veterans and the Substance Abuse and Mental Health Services Administration estimates that about seven percent of veterans have a substance abuse disorder.

(b) FINDINGS.—Congress makes the following findings:

(1) Our ally Israel, under constant attack from terrorist groups, experiences similar issues with Israeli veterans facing symptoms of PTSD. The National Center for Traumatic Stress and Research at Tel Aviv University found that five to eight percent of combat soldiers experience some form of PTSD, and during wartime, that figure rises to 15 to 20 percent.

(2) Current treatment options in the United States focus on cognitive therapy, exposure therapy, or eye movement desensitization and reprocessing, but the United States must continue to look for more effective treatments. Several leading hospitals, academic institutions, and nonprofit organizations in Israel have conducted research and services to treating PTSD.

(3) SENSE OF CONGRESS.—It is the sense of Congress that the Secretary of Defense, acting through the Psychological Health and Traumatic Brain Injury Research Program, should seek to explore scientific collaborations between academic institutions and nonprofit research entities in the United States and institutions in Israel with expertise in researching, diagnosing, and treating post-traumatic stress disorder.

(c) AMENDMENT.—The Secretary of Defense shall carry out the grant program under this section in accordance with the Agreement on the United States-Israel binational science foundation with exchange of letters, signed at New York September 27, 1972, and entered into force on September 27, 1972.

(d) ELIGIBILITY.—To be eligible to receive a grant under this section, an entity shall be an academic institution or a nonprofit entity located in the United States.

(e) AWARD.—The Secretary shall award grants under this section to eligible entities that—

(1) carry out a research project that—

(A) addresses a requirement in the area of post-traumatic stress disorders that the Secretary determines appropriate to research using such grant; and

(B) is conducted by the eligible entity and an entity in Israel under a joint research agreement; and

(2) meet such other criteria that the Secretary may establish.

(f) APPLICATION.—To be eligible to receive a grant under this section, an eligible entity shall submit an application to the Secretary at such time, in such manner, and containing such commitments and information as the Secretary may require.

(g) REQUIRED REPORT.—Not later than 60 days after the date on which an eligible entity completes a research project using a grant under this section, the Secretary shall submit to Congress a report that contains—

(A) a description of the research project;

(B) an evaluation of the level of success of the research project;

(C) the length of time required to process each claim, as measured from the date on which the claim is filed to the final disposition of the claim; and

(D) the number of claims filed under this subtitle.

SEC. 3681A. COMPLETION AND UPDATES OF SITE EXPOSURE MATRICES.

(a) DEFINITION.—In this section, the term ‘‘site exposure matrices’’ means an exposure assessment of a Department of Energy facility that identifies the toxic substances or processes that were used in each building or process of the facility, including the trade names (if any) of the substance.

(b) IN GENERAL.—Not later than 180 days after the date of enactment of the Toxic Exposure Safety Act of 2021, the Secretary of Labor shall, in consultation with the Secretary of Energy, create or update site exposure matrices for each Department of Energy facility based on the records, files, and other data provided by the Secretary of Energy and such other information as is available, including information available from the former worker medical screening programs on the Department of Energy’s website and any other database used by the Secretary of Labor to evaluate claims for compensation under this title; and other data provided by the Secretary of Energy and each Department of Energy facility, regarding—

(1) the site exposure matrices, as periodically updated under subsections (b) and (c); and

(2) each site profile prepared under section 3683(a).

(c) PERIODIC UPDATE.—Beginning 90 days after the initial creation or update described in subsection (b), and each 90 days thereafter, the Secretary shall update the site exposure matrices with all information available as of such time from the Secretary of Energy.

(d) INFORMATION.—The Secretary of Energy shall furnish to the Secretary of Labor any information that the Secretary of Labor finds necessary or useful for the production or updating of the site exposure matrices for this section, including records from the Department of Energy former worker medical screening programs.

(e) PUBLIC AVAILABILITY.—The Secretary of Labor shall make available to the public, on the primary website of the Department of Labor,—

(1) the site exposure matrices, as periodically updated under subsections (b) and (c); and

(2) each site profile prepared under section 3683(a).

(f) INFORMATION.—Any other database used by the Secretary of Labor to evaluate claims for compensation under this title; and other statistical data shall be aggregate and disaggregated by each Department of Energy facility, regarding—

(A) the number of claims filed under this subtitle;

(B) the types of illnesses claimed;

(C) the number of claims filed for each type of illness and, for each claim, whether the claim was approved or denied; and

(D) the length of time required to process each claim, as measured from the date on which the claim is filed to the final disposition of the claim.

(g) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Secretary of Energy, for fiscal year 2022 and each succeeding year, such sums as may be
necessary to support the Secretary of Labor in creating or updating the site exposure matrices.”.

SEC. 3163. ASSISTING CURRENT AND FORMER EMPLOYEES UNDER THE EOCPCA.

(a) PROVIDING INFORMATION AND OUTREACH.—Subtitle A of the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7384l et seq.) is amended—

(1) by redesigning section 3614 as section 3616; and

(2) by inserting after section 3613 the following:

**SEC. 3614. INFORMATION AND OUTREACH.**

"(a) ESTABLISHMENT OF TOLL-FREE INFORMATION PHONE NUMBER.—By not later than January 1, 2023, the Secretary of Labor shall establish a toll-free phone number that current or former employees of the Department of Energy, or current or former Department of Energy contractor employees, may use in order to receive information regarding—

"(1) the compensation program under subtitle B or E;

"(2) information regarding the process of submitting a claim under either compensation program;

"(3) assistance in completing the occupational health questionnaire required as part of a claim under subtitle B or E;

"(4) the next steps to take if a claim under subtitle B or E is accepted or denied; and

"(5) information as the Secretary determines necessary to further the purposes of this title.

"(b) ESTABLISHMENT OF RESOURCE AND ADVOCACY CENTER.—

"(1) IN GENERAL.—By not later than January 1, 2023, the Secretary of Energy, in coordination with the Secretary of Labor, shall establish a resource and advocacy center at each Department of Energy facility where cleanup operations are being carried out, or have been carried out, under the environmental management program of the Department of Energy. Each such resource and advocacy center shall assist current or former Department of Energy employees and current or former Department of Energy contractor employees, by enabling the employees and contractor employees to—

"(A) obtain information regarding all related programs available to them relating to potential claims under this title, including—

"(i) programs under subtitles B and E; and

"(ii) other medical or monitoring programs of the Department of Energy; and

"(B) navigate all such related programs.

"(2) COORDINATION.—The Secretary of Energy shall integrate other programs available to current and former employees, and current or former Department of Energy contractor employees, which are related to the purposes of this title, with the resource and advocacy centers established under paragraph (1), as appropriate.

"(c) INFORMATION.—The Secretary of Labor shall develop and distribute, through the resource and advocacy centers established under subsection (b) and other means, information (which may include responses to frequently asked questions) for current or former employees or current or former Department of Energy contractor employees about the programs under subtitles B and E and the process under such programs.

"(d) COPY OF EMPLOYEE’S CLAIMS RECORDS.—

"(1) IN GENERAL.—The Secretary of Labor shall, upon the request of a current or former employee or Department of Energy contractor employee, provide the employee with a complete copy of all records or other materials held by the Department of Energy or Department of Energy contractor employees relating to the employee’s claim under subtitle B or E.

"(2) CHOICE OF FORMAT.—The Secretary of Labor shall provide the copy of records described in paragraph (1) to an employee in electronic or paper form, as selected by the employee.

"(e) CONTACT OF EMPLOYEES BY INDUSTRIAL HYGIENISTS.—The Secretary of Labor shall allow industrial hygienists to contact and provide counseling, education, and training to employees or contractor employees of the Department of Energy or contractor employees regarding the employee’s claim under subtitle B or E.

"(f) EXTENDING APPEAL PERIOD.—Section 3677(a) of the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7384s–3) is amended by striking ‘‘60 days’’ and inserting ‘‘180 days’’.

"(g) FUNDING.—Section 3684 of the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7384s–13) is amended—

"(1) by striking ‘‘There is authorized to be appropriated to the Secretary of Energy for fiscal year 2023 and each succeeding year such sums as may be necessary to support the Secretary in carrying out the requirements of this section’’; and

"(2) by adding at the end the following:

"(‘‘(b) ADMINISTRATIVE COSTS FOR DEPARTMENT OF ENERGY.—There is authorized to be appropriated to the Secretary of Energy for fiscal year 2023 and each succeeding year such sums as may be necessary to support the Secretary in carrying out the requirements of this section’’);

"(d) ADVISORY BOARD ON TOXIC SUBSTANCES AND WORKER HEALTH.—Section 3687 of the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7384s–16) is amended—

"(1) in subsection (b)—

"(A) in paragraph (1)(F), by striking ‘‘and’’ after the semicolon;

"(B) in paragraph (2), by striking the period at the end and inserting a semicolon; and

"(C) by adding at the end the following:

"‘‘(3) develop recommendations for the Secretary of Health and Human Services regarding whether there is a class of Department of Energy employees, Department of Energy contractor employees, or other employees at any Department of Energy facility who were at least as likely as not exposed to toxic substances that they would have been exposed to if they were not feasible to estimate with sufficient accuracy the dose they received; and

"(4) review all existing, as of the date of the report, rules and guidelines issued by the Secretary regarding presumption of causation and provide the Secretary with recommendations for new rules and guidelines regarding presumption of causation.’’;

"(2) in subsection (c)(3), by inserting ‘‘or the Board’’ after ‘‘The Secretary’’;

"(3) by redesignating subsections (b), (1), and (i) as subsections (i), (j), and (k), respectively; and

"(4) by inserting after subsection (g) the following:

‘‘(h) REQUIRED RESPONSES TO BOARD RECOMMENDATIONS.—Not later than 90 days after the date on which the Secretary of Labor and the Secretary of Health and Human Services receive recommendations in accordance with paragraph (1), (3), or (4) of subsection (b), each such Secretary shall submit formal responses to each recommendation to the Board and Congress. ’’

SEC. 3164. RESEARCH PROGRAM ON EPIDEMIOLOGICAL IMPACTS OF TOXIC EXPOSURES.

(a) DEFINITIONS.—In this section—

"(1) the term ‘‘Department of Energy facility’’ has the meaning given the term in section 703 of the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7384l); and

"(2) the term ‘‘institution of higher education’’ has the meaning given such term in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001); and

"(3) the term ‘‘Secretary’’ means the Secretary of Health and Human Services.

(b) ESTABLISHMENT.—The Secretary, acting through the Director of the National Institutes of Health and in collaboration with the Director of the Centers for Disease Control and Prevention, shall conduct or support research on the epidemiological impacts of toxic substances at Department of Energy facilities.

(c) USE OF FUNDS.—Research under subsection (a) may include research on the epidemiological, clinical, or health impacts on individuals who were exposed to toxic substances in or near the tank or other storage farms and other relevant Department of Energy facilities through their work at such sites.

(d) ELIGIBILITY AND APPLICATION.—Any institution of higher education or the National Academy of Sciences may apply for funding under this section by submitting to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require.

(e) RESEARCH COORDINATION.—The Secretary shall coordinate with the institution of higher education that submits an application for research under this section with similar activities conducted by the Department of Health and Human Services to the extent that other agencies have responsibilities that are related to the study of epidemiological, clinical, or health impacts of exposures to toxic substances.

(f) HEALTH STUDIES REPORT TO SECRETARY.—Not later than 1 year after the end of the funding period for research under this section, the funding recipient shall prepare and submit to the Secretary a final report that—

"(1) summarizes the findings of the research;

"(2) includes recommendations for any additional studies;

"(3) describes any classes of employees that, based on the results of the report, could warrant the establishment of a Special Exposure Registry under the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7384 et seq.) for toxic substance exposures; and

"(4) identifies any illnesses to be included as covered illnesses under such Act (42 U.S.C. 7384 et seq.).

(g) REPORT TO CONGRESS.—(1) IN GENERAL.—Not later than 120 days after the date on which the reports under subsection (f) are due, the Secretary shall—

"(A) identify a list of cancers and other illnesses associated with toxic substances that pose, or posed, a hazard in the work environment at any Department of Energy facility;

"(B) prepare and submit to the relevant committees of Congress a report—

"(i) summarizing the findings from the reports required under subsection (f); and

"(ii) identifying any new illnesses that, as a result of the study, will be included as covered illnesses, pursuant to subsection (f)(4) and section 3671(2) of the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7384(2)); and

"(iii) including the Secretary’s recommendations for additional health studies relating to toxic substances, if the Secretary determines it necessary.

(2) RELEVANT COMMITTEES OF CONGRESS DEFINED.—In this section, the term ‘‘relevant committees of Congress’’ means—

"(A) the Committee on Armed Services, Committee on Appropriations, Committee on
Energy and Natural Resources, and Committee on Health, Education, Labor, and Pensions of the Senate; and

(b) the Committee on Armed Services, Committees, Committee on Energy and Commerce, and Committee on Education and Labor of the House of Representatives.

(2) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this section $3,000,000 for each of fiscal years 2022 through 2026.

SEC. 3165. NATIONAL ACADEMY OF SCIENCES REVIEW.

Subtitle A of the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7384 et seq.), as amended by section 3163, is further amended by inserting after section 3164 the following:

"SEC. 3165. NATIONAL ACADEMY OF SCIENCES REVIEW.

"(a) PURPOSE.—The purpose of this section is to enable the National Academy of Sciences, a non-Federal entity with appropriate expertise, to review and evaluate the available scientific evidence regarding associations between diseases and exposure to toxic substances found at Department of Energy cleanup sites.

"(b) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to enable the National Academy of Sciences, not later than 60 days after the issuance of the health studies report, to carry out the requirements of this section.

"(c) AGREEMENT.—The Secretary of Energy and Human Services shall seek to enter into an agreement with the National Academy of Sciences, not later than 60 days after the issuance of the health studies report, to carry out the requirements of this section.

"(d) REVIEW OF SCIENTIFIC AND MEDICAL EVIDENCE.—

"(1) IN GENERAL.—Under the agreement described in subsection (c), the National Academy of Sciences shall, for the period of the agreement:

"(A) for each area recommended for additional study under the health studies report submitted under subsection (f) of the Toxic Exposure Safety Act of 2021, review and summarize the scientific evidence relating to the area, including—

"(i) studies by the Department of Energy and Department of Labor; and

"(ii) any other available and relevant scientific evidence, to the extent that such studies are relevant to the occupational exposures that have occurred at Department of Energy cleanup sites and

"(B) review and summarize the scientific and medical evidence concerning the association between exposure to toxic substances found at Department of Energy cleanup sites and resultant diseases.

"(2) SCIENTIFIC DETERMINATIONS CONCERNING DISEASES.—In conducting each review of scientific evidence under subparagraphs (A) and (B) of paragraph (1), the National Academy of Sciences shall—

"(A) assess the state of such evidence;

"(B) assess whether a statistical association between exposure to a toxic substance and a disease exists, taking into account the strength of such association, the scientific evidence and the appropriateness of the statistical and epideimologic methods used to detect an association;

"(C) assess the increased risk of disease among those exposed to the toxic substance during service during the production and cleanup eras of the Department of Energy cleanup sites;

"(D) survey the impact to health of the toxic substance, focusing on hematologic, gastrointestinal, neurologic, dermatologic, respiratory, endocrine, ocular, ear, nasal, and oropharyngeal diseases, including dementia, leukemia, chemical sensitivity, and chronic obstructive pulmonary disease; and

"(E) determine whether a plausible biological mechanism or other evidence of a causal relationship exists between exposure to the toxic substance and disease.

"(e) ADDITIONAL SCIENTIFIC STUDIES.—If the National Academy of Sciences determines, in the course of carrying out the studies under subsection (d), that additional studies are needed to resolve areas of continuing scientific uncertainty relating to toxic exposure at Department of Energy cleanup sites, the National Academy of Sciences shall include, in the next report submitted under subsection (f), recommendations for areas of additional study, consisting of—

"(1) a list of diseases and toxins that require further evaluation and study;

"(2) a review of the available information, as of the date of the report, relating to such diseases and toxins;

"(3) the value of the information that would result from additional studies; and

"(4) the cost and feasibility of carrying out additional studies.

"(f) REPORTS.—

"(1) IN GENERAL.—By not later than 18 months after the date of the agreement under subsection (c), and every 2 years thereafter, the National Academy of Sciences shall submit an agreement prepare and submit a report to—

"(A) the Secretary;

"(B) the Committee on Health, Education, Labor, and Pensions and the Committee on Energy and Natural Resources of the Senate; and

"(C) the Committee on National Resources, the Committee on Education and Labor, and the Committee on Energy and Commerce of the House of Representatives.

"(2) CONTENTS.—Each report submitted under paragraph (1) shall include—

"(i) the reviews and studies conducted under this section;

"(ii) the determinations and conclusions of the National Academy of Sciences with respect to such reviews and studies; and

"(iii) the scientific evidence and reasoning that led to such conclusions;

"(B) the recommendations for further areas of study made under subsection (e) for the reporting period;

"(C) a description of any classes of employees that, based on the results of the reviews and studies, could qualify as a Special Exposure Cohort;

"(D) the identification of any illness that the National Academy of Sciences has determined, as a result of the reviews and studies, should be covered an illness.

"(g) LIMITATION ON AUTHORITY.—The authority to enter into agreements under this section shall be effective for a fiscal year to the extent that appropriations are available.

"(h) SUNSET.—This section shall cease to be effective 18 months after the last day of the fiscal year in which the National Academy of Sciences transmits to the Secretary the first report under subsection (f)."

"SEC. 3166. CONFORMING AMENDMENTS.

"(a) The Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7384 et seq.) is amended—

"(1) in the table of contents—

"(A) by redesignating the item relating to section 3614 as the item relating to section 3616; and

"(B) by inserting after the item relating to section 3613 the following:

"‘‘Sec. 3614. Information and outreach.

‘‘Sec. 3615. National Academy of Sciences review.’’;

"(B) by inserting after the item relating to section 3681 the following:

"‘‘Sec. 3681A. Completion and updates of site exposure matrices.’’;

"(C) by inserting after the item relating to section 3681 the following:

"‘‘Sec. 3681A. Completion and updates of site exposure matrices.’’;

"and

"(2) in each of subsections (b)(1) and (c) of section 3612, by striking ‘‘3614(b)’’ and inserting ‘‘3615(b)’’.

"SA 4793. Mr. LEE (for himself and Mr. DAINES) submitted an amendment intended to be proposed to amendment SA 47 submitted by Mr. Reed and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 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:

In section 511, beginning in subsection (d)(4), strike the period at the end of sub-paragraph (B)(ii) and all that follows through subsection (g) and insert the following: ‘‘;

"(g) No person may be inducted for training and service under this title if such person—

"(1) has a dependent child and the other parent of the dependent child has been inducted for training or service under this title or the person volunteers for such induction;

"(2) has a dependent child who has no other living parent.

"Section 10(b)(3) (50 U.S.C. 3809(b)(3)) is amended by striking ‘‘the President is requested’’ and all that follows through ‘‘race or national origin’’ and inserting ‘‘the President is requested to approve the appointment of each local board so that each board has both male and female members and, to the maximum extent practicable, is proportionately representative of those registrants within its jurisdiction in each applicable basis set forth in section 703(a) of the Civil Rights Act of 1964 (42 U.S.C. 2000e–2(a)), but no action by any board shall be declared invalid on the ground that such board failed to conform to such representation quota’’;

"(6) Section 16(a) (50 U.S.C. 3814(a)) is amended by striking ‘‘men’’ and inserting ‘‘persons’’;

"(7) Section 16(a)(1) (50 U.S.C. 3800(a)(1)) is amended by striking ‘‘persons’’.

"(e) MAINTAINING THE HEALTH OF THE SELECTIVE SERVICE SYSTEM.—Section 16(a) (50 U.S.C. 3800(a)) is amended by adding at the end the following new paragraph:

"(2) The Selective Service System shall conduct exercises periodically of all mobilization plans, systems, and processes to evaluate and test the effectiveness of such plans, systems, and processes. Once every 4 years, the exercise shall include the full range of internal and external procedures to ensure functionality and interoperability and may take place as part of the Department of Defense mobilization exercise under section 15 of title 10, United States Code. The Selective Service System shall conduct a public awareness campaign in conjunction
with each exercise to communicate the purpose of the exercise to the public.

(f) TECHNICAL AND CONFORMING AMENDMENTS.—The Military Selective Service Act is amended—

(i) in section 4 (50 U.S.C. 3803)—

(A) in subsection (a) in the third undesignated paragraph—

(1) by striking “such his acceptability in all respects, including
such person’s” and inserting “such person’s acceptability in all respects, including
such person’s” and

(ii) by striking “he may prescribe” and inserting

“the President may prescribe”;

(B) in subsection (c)—

(i) in paragraph (2), by striking “any en-
listed member” and inserting “any person
who is an enlisted member”;

(ii) in paragraphs (3), (4), and (5), by strik-
ing “in which he resides” and inserting “in
which such person resides”;

(C) in subsection (d), by striking “coordinate
with him” and inserting “coordinate
with the Director”;

(D) in subsection (k)(1), by striking “find-
ing by him” and inserting “finding by the
President”;

(ii) in section 5(d) (50 U.S.C. 3805(d)), by striking “he may prescribe” and inserting

“the President may prescribe”;

(iii) in section 6 (50 U.S.C. 3806)—

(A) in subsection (c)(2)(D), by striking “he may
determine” and inserting “the President
considers appropriate”;

(B) in subsection (d)(3), by striking “he may
determine” and inserting “the President
consider determines appropriate”;

(C) in subsection (h), by striking “he may
prescribe” each place it appears and insert-
ing “the President may prescribe”;

(iv) in section 10 (50 U.S.C. 3809)—

(A) in subsection (b)—

(i) in paragraph (3)—

(I) by striking “He shall create” and in-
serting “the President shall create”;

(II) by striking “upon his own motion” and
inserting “upon the President’s own
motion”;

(ii) in paragraph (4), by striking “his sta-
tus” and inserting “such individual’s sta-
tus”;

(iii) in paragraphs (6), (8), and (9), by strik-
ing “he may determine” each place it ap-
pers and inserting “the President con-
siders”;

(B) in subsection (c), by striking “vested in
him” and inserting “vested in the President”;

(v) in section 13(b) (50 U.S.C. 3812(b)), by striking “regulation if he” and inserting

“regulation if the President”;

(B) in subsection (a), by striking “Upon the
President’s” and inserting “the President’s”;

(B) in subsection (b), by striking “he may
determine” each place it appears and insert-
ing “the President considers”;

(C) in subsection (d), by striking “he may
determine” and inserting “the President
considers”;

(ii) in section 16(g) (50 U.S.C. 3814(g))—

(A) in paragraph (1), by striking “who as
his regular and customary vocation” and in-
serting “who, as such person’s regular and customary vocation”;

(B) in paragraph (2)—

(i) by striking “one who as his customary
vocation” and inserting “a person who, as
such person’s customary vocation,” and

(ii) by striking “he is a member” and in-
serting “such person is a member”;

(B) in section 18(a) (50 U.S.C. 3816(a)), by strik-
ing “National” and inserting “the Presi-
dent is authorized”;

(C) in section 21 (50 U.S.C. 3819)—

(A) by striking “he is sooner” and insert-
ing “he is sooner”;

(B) by striking “he” each subsequent place it appears and inserting “such member”; and

(C) by striking “his consent” and inserting

“such member’s consent”;

(10) in section 22(b) (50 U.S.C. 3820(b)), in paragraphs (1) and (2), by striking “his” each
place it appears and inserting “the reg-
istrant’s”; and

(11) except as otherwise provided in this section—

(A) by striking “be” each place it appears and insert-
ing “such person”;

(B) by striking “his” each place it appears and insert-
ing “such person’s”;

(C) by striking “be” each place it appears and insert-
ing “such person”;

(D) by striking “present himself” each
place it appears in section 12 (50 U.S.C. 3811)
and inserting “present himself”.

(g) ENACTMENT OF AUTHORIZATION RE-
QUIRED FOR DRAFT.—

(I) FINDINGS.—Congress makes the fol-
lowing findings:

(A) Clause 12 of section 8 of article I of the
Constitution of the United States empowers
Congress with the responsibility to “raise
and support Armies”.

(B) The United States first required mili-
tary conscription in the American Civil War
under the Civil War Military Draft Act of 1862.

(C) The Selective Services Act of 1917 au-
thorized the President to draft additional
forces beyond the number imposed by the
exceedingly high demand for additional
forces when the U.S. entered the first World
War.

(D) The Selective Training and Service Act
of 1940 was the first authorization by Con-
gress for conscription in peacetime but lim-
lited the President’s induction authority to
no greater number of men than the Con-
gress shall hereafter make specific approp-
riation for from time to time”.

(E) Congress allowed induction authority
to lapse in 1945.

(F) Congress reinstated the President’s in-
duction authority under the Selective Serv-
ice Act of 1948 to raise troops for United
States participation in the Korean War.

(G) Congress maintained the President’s
induction authority under the Selective
Service Act of 1948 through the beginning
of the Vietnam War.

(H) Congress passed additional reforms to
the draft under the Military Selective Serv-
ice Act of 1967 in response to issues arising
from United States engagement in the Viet-
nam War.

(I) Congress prohibited any further use of
the draft after July 1, 1973.

(J) If a president seeks to reactivate the
use of the draft, Congress would have to
enact a law providing authorization for this
purpose.

(AMENDMENT.—Section 17 of the Military
Selective Service Act (50 U.S.C. 3815) is
amended by adding at the end the following
new subsection:

(‘‘(d) No person shall be inducted for train-
ing and service in the Armed Forces unless
Congress first passes and there is enacted a
law expressly authorizing such induction
into service.’’.

(EFFECTIVE DATE.—The amendments
made by this section shall take effect on the
date of the enactment of this Act, except
that the amendments made by subsections
(d) and (g) shall take effect 1 year after such
date of enactment.

SA 4794. Mr. RISCH (for himself, Mr.
PORTMAN, Mr. CRUZ, Mr. BARRASSO, Mr.
JOHNSON, Mr. COTTON, and Mr. DAINES)
submitted an amendment intended to
be proposed to amendment SA 3867 sub-
mitted by Mr. REED and intended to be
proposed to the bill H.R. 4350, to au-
thorize appropriations for fiscal year
2022 for military activities of the De-
partment of Defense, for military con-
struction, 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;
and

At the end of subtitle D of title XII, add
the following:

SEC. 1237. IMPOSITION OF SANCTIONS WITH
RESPECT TO NORD STREAM 2.

(a) IN GENERAL.—Not later than 15 days af-
after the date of the enactment of this Act,
the President shall—

(1) impose sanctions under subsection (b)
with respect to any corporate officer of an
entity established for or responsible for
the planning, construction, or operation of
the Nord Stream 2 pipeline or a successor
entity;

(b) INELIGIBILITY FOR VISAS, ADMISSION, OR
PAROLE OF IDENTIFIED PERSONS AND COR-
PORATE OFFICERS.—

(I) GENERAL.—(A) VISAS, ADMISSION, OR PAR-
ROLE.—An alien described in subsection (a)(1) is

(i) ineligible to be admitted or
paroled into the United States;

(ii) ineligible to receive a visa or other doc-
tumentation to enter the United States; and

(iii) otherwise ineligible to be admitted or
paroled into the United States or to receive
any other benefit under the Immigration and
Nationality Act (8 U.S.C. 1101 et seq.).

(B) CURRENT VISAS REVOKED.—

(i) IN GENERAL.—The visa or other entry
documentation of an alien described in sub-
section (a)(1) shall be revoked, regardless of
when such visa or other entry documenta-
tion is or was issued.

(ii) IMMEDIATE EFFECT.—A revocation under
clause (i) shall—

(I) take effect immediately; and

(II) automatically cancel any other valid
visa or entry documentation that is in
the alien’s possession.

(c) BLOCKING OF PROPERTY OF IDENTIFIED
PERSONS AND CORPORATE OFFICERS.—The President shall exercise all
powers granted to the President by the
International Emergency Economic Powers
Act (50 U.S.C. 1701 et seq.) to the extent nec-
cessary to permit the United States to
enforce all laws and regulations, including
sanctions, with respect to any entity described in subsection (a)(1) if
such property and interests in property of
an entity described in subsection (a)(1) are
within the United States, are or are come
within the possession or control of a United
States person.

(d) EXCEPTIONS.—

(I) EXCEPTION FOR INTELLIGENCE, LAW EN-
FORCEMENT, AND NATIONAL SECURITY ACTI-
VITIES.—Sanctions under this section shall not
apply to any authorized intelligence, law en-
forcement, or national security activities of
the United States.

(2) EXCEPTION TO COMPLY WITH UNITED NA-
TIONS HEADQUARTERS AGREEMENT.—Sanctions
under this section shall not apply with re-
spect to the admission of an alien to the
United States if the admission of the alien is
necessary to permit the United States to
comply with the Agreement regarding the
Headquarters of the United Nations, signed
at Lake Success June 26, 1947, and entered
into force November 21, 1947, between the
United Nations and the United States, the
Convention on Consular Relations, done at
Vienna April 24, 1963, and entered into force
March 19, 1967, or other applicable inter-
national obligations.

(3) EXCEPTION RELATING TO IMPORTATION OF
GOODS—
(A) in general.—Notwithstanding any other provision of this section, the authorities and requirements to impose sanctions under this section shall not include the authority or requirement to impose sanctions on the importation of goods.

(B) good defined.—In this paragraph, the term ‘‘good’’ means any article, natural or man-made, material, supply or manufactured product, including inspection and test equipment, and excluding technical data.

SEC. 1239. APPLICATION OF CONGRESSIONAL REVIEW UNDER COUNTERING AMERICA’S ADVERSARIES THROUGH SANCTIONS ACT.

Section 216(a)(2) of the Countering America’s Adversaries Through Sanctions Act (22 U.S.C. 9511(a)(2)) is amended—

(1) in subparagraph (A), in clause (I), by striking ‘‘other than sanctions described in clause (I)(IV) of that subparagraph’’ after ‘‘subparagraph (B);’’ and

(2) in clause (II), by striking ‘‘or otherwise remove’’ after ‘‘waive;’’ and

(B) in clause (III), by striking ‘‘and’’ and inserting a semicolon;

(C) in subsection (B), by striking ‘‘Continued’’ and inserting—

‘‘(IV) section 7503 of the Protecting Europe’s Energy Security Act of 2019 (title LXXV of Public Law 116–92; 22 U.S.C. 9526 note); or

‘‘(V) section 1237 of the National Defense Authorization Act for Fiscal Year 2022; and’’.

SEC. 1240. INCLUSION OF MATTER RELATING TO NORD STREAM 2 IN REPORT UNDER COUNTERING AMERICA’S ADVERSARIES THROUGH SANCTIONS ACT.

Each report submitted under section 216(a)(1) of the Countering America’s Adversaries Through Sanctions Act (22 U.S.C. 9511(a)(1)) shall include—

(1) an assessment of the security risks posed by Nord Stream 2, including—

(A) the presence along Nord Stream 2 or Nord Stream 1 infrastructure of entities that are involved in the design, engineering, 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; and

(B) in subclause (II), by striking ‘‘; or’’ and

(c) sunset.—The authority to impose sanctions under this section shall terminate on the date that is 5 years after the date of the enactment of this Act.

(d) definitions.—In this section—

(1) admission; admitted; alien.—The terms ‘‘admission’’, ‘‘admitted’’, and ‘‘alien’’ have the meanings given those terms in section 101 of the Immigration and Nationality Act (8 U.S.C. 1101).

(2) appropriate congressional committees—

(A) the Committee on Foreign Relations and the Committee on Banking, Housing, and Urban Affairs of the Senate; and

(B) the Committee on Foreign Affairs and the Committee on Financial Services of the House of Representatives.

(3) united states person.—The term ‘‘United States person’’ means—

(A) a United States citizen or an alien lawfully admitted for permanent residence to the United States; and

(B) an entity organized under the laws of the United States or any jurisdiction within the United States including a foreign branch of such an entity; or

(C) any person within the United States.

SEC. 1238. CONGRESSIONAL REVIEW OF WAIVER UNDER PROTECTING EUROPE’S ENERGY SECURITY ACT OF 2019.

Section 7503(f) of the Protecting Europe’s Energy Security Act of 2019 (title LXXV of Public Law 116–92; 22 U.S.C. 9526 note) is amended, in the matter preceding paragraph (1), by striking ‘‘The President’’ and inserting ‘‘Subject to review by Congress under section 216(a)(2) of the Countering America’s Adversaries Through Sanctions Act (22 U.S.C. 9511(a)(2)), the President’’.
from any military construction program authorized by any Act to authorize appropriations for a fiscal year for military activities of the Department of Defense and for military construction.

(c) NAVY PUBLIC SHIPYARD DEFINED.—In this section, the term "Navy public shipyard" means the

1. The Norfolk Naval Shipyard, Virginia.
2. The Pearl Harbor Naval Shipyard, Hawaii.
3. The Portsmouth Naval Shipyard, Maine.

SA 4796. Mr. PAUL submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 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 fiscal year 2022, and for other purposes; which was ordered to lie on the table; as follows:

At the end of title C of title VII, add the following:

SEC. 744. PROHIBITION ON DISHONORABLE DISCHARGE TO A MEMBER OF THE ARMED FORCES FOR REFUSING TO COMPLY WITH COVID–19 VACCINE MANDATE.

The Secretary of Defense may not give a dishonorable discharge to a member of the Armed Forces solely on the basis of the refusal of the member, for religious, medical, or personal reasons, to comply with any requirement that the member receive a vaccination for coronavirus disease 2019 (commonly known as "COVID–19").

SA 4797. Mr. BENNET submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 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 fiscal year 2022, and for other purposes; which was ordered to lie on the table; as follows:

At the end of title D of title XVIII, add the following:

SEC. 2836. PAYMENT TO ENVIRONMENTAL PROTECTION AGENCY FOR CERTAIN COSTS IN CONNECTION WITH FORMER ROCKY MOUNTAIN ARSENAL, COLORADO.

(a) AUTHORITY FOR PAYMENT.—

(1) TRANSFER AMOUNT.—

(A) In general.—In subsection 2215 of title 10, United States Code, chapter 169 of such title, section 1367 of the National Defense Authorization Act for Fiscal Year 1987 (Public Law 99–661; 100 Stat. 4003), or any other provision of law, using funds described in subsection (b), the Secretary of Defense may transfer to the Administrator of the Environmental Protection Agency for use at the former Rocky Mountain Arsenal, Colorado—

1. In fiscal year 2022, $1,805,000 for costs associated with the involvement of the Environmental Protection Agency with the cleanup by the Department of the Army of the former Rocky Mountain Arsenal from fiscal year 2019 through fiscal year 2020, after a specific accounting is provided in accordance with subparagraph (B); and

SEC. 2836. PAYMENT TO ENVIRONMENTAL PROTECTION AGENCY FOR CERTAIN COSTS IN CONNECTION WITH FORMER ROCKY MOUNTAIN ARSENAL, COLORADO.

(a) AUTHORITY FOR PAYMENT.—

(1) TRANSFER AMOUNT.—

(A) In general.—In subsection 2215 of title 10, United States Code, chapter 169 of such title, section 1367 of the National Defense Authorization Act for Fiscal Year 1987 (Public Law 99–661; 100 Stat. 4003), or any other provision of law, using funds described in subsection (b), the Secretary of Defense may transfer to the Administrator of the Environmental Protection Agency for use at the former Rocky Mountain Arsenal, Colorado—

1. In fiscal year 2022, $1,805,000 for costs associated with the involvement of the Environmental Protection Agency with the cleanup by the Department of the Army of the former Rocky Mountain Arsenal from fiscal year 2019 through fiscal year 2020, after a specific accounting is provided in accordance with subparagraph (B); and
(2) by inserting after subsection (k) the following:

"(l) Postsecondary Student Data System—

"(1) IN GENERAL.—

"(A) ESTABLISHMENT OF SYSTEM.—Not later than 4 years after the date of enactment of the College Transparency Act, the Commissioner of the National Center for Education Statistics (referred to in this subsection as the ‘Commissioner’) shall develop and maintain the postsecondary student-level federal data system for the purposes of:

(i) accurately evaluate student enrollment, completion, and postgraduate outcomes, and higher education costs and financial aid;

(ii) assist with transparency, institutional improvement, and analysis of Federal aid programs;

(iii) provide accurate, complete, and customizable information for students and families making decisions about postsecondary education; and

(iv) reduce the reporting burden on institutions of higher education, in accordance with section 5(b) of the College Transparency Act.

"(B) AVOIDING DUPLICATED REPORTING.—Notwithstanding any other provision of this section, to the extent that another provision of this section requires the same reporting or collection of data that is required under this subsection, an institution of higher education, or the Secretary or Commissioner, may use the reporting or data required for the postsecondary student data system under this subsection to satisfy both requirements.

"(C) DEVELOPMENT PROCESS.—In developing the postsecondary student data system described in this subsection, the Commissioner shall—

(i) focus on the needs of—

(A) users of the data system; and

(B) entities, including institutions of higher education, reporting to the data system;

(ii) take into consideration, to the extent practicable—

(A) the guidelines outlined in the U.S. Web Design Standards maintained by the General Services Administration and the Digital Services Playbook and TechFAIR Handbook for Procuring Digital Services Using Agile Processes of the U.S. Digital Service; and

(B) any successor documents or recommendations of such guidelines;

(iii) use modern, relevant privacy- and security-enhancing technology, and enhance and update the system as necessary to carry out the purpose of this subsection;

(iv) ensure data privacy and security is consistent with any Federal law relating to privacy or data security, including—

(A) the requirements of subchapter II of chapter 5 of title 44, United States Code, specifying security categorization under the Federal Information Processing Standards or any relevant successor of such standards;

(B) security requirements that are consistent with the Federal agency responsibilities in section 3554 of title 44, United States Code, or any relevant successor of such responsibilities; and

(C) security requirements, guidelines, and controls consistent with cybersecurity standards and best practices developed by the National Institute of Standards and Technology, including frameworks, consistent with section 1402 of the National Institute of Standards and Technology Act (15 U.S.C. 272(c)), or any relevant successor of such frameworks;

(v) provide for the Federal data minimization practices to ensure only the minimum amount of data is collected to meet the system’s goals, in accordance with Federal data minimization standards and guidelines developed by the National Institute of Standards and Technology; and

(vi) provide for student-related surveys outlining the data included in the system and how the data are used.

"(2) DATA ELEMENTS.—

"(A) IN GENERAL.—Not later than 4 years after the date of enactment of the College Transparency Act, the Commissioner, in consultation with the Postsecondary Student Data System Advisory Committee established under subparagraph (B), shall determine—

(i) the data elements to be included in the postsecondary student data system, in accordance with subparagraphs (C) and (D); and

(ii) how to include the data elements required under subparagraph (C), and any additional data elements selected under subparagraph (D), in the postsecondary student data system.

"(B) POSTSECONDARY STUDENT DATA SYSTEM ADVISORY COMMITTEE.—

"(1) ESTABLISHMENT.—Not later than 2 years after the date of enactment of the College Transparency Act, the Commissioner shall establish a Postsecondary Student Data System Advisory Committee (referred to in this subsection as the ‘Advisory Committee’), whose members shall—

(I) the Chief Privacy Officer of the Department of Education or an official of the Department delegated the duties of overseeing data privacy at the Department;

(II) the Chief Security Officer of the Department or an official of the Department delegated the duties of overseeing data security at the Department;

(III) representatives of diverse institutions of higher education, which shall include institutions of higher education, the Secretary, or the Commissioner, and the Secretary or Commissioner, as specified in this subsection, the Commissioner, shall ensure that the Advisory Committee—

(I) the data elements to be included in the postsecondary student data system, in accordance with subparagraph (C) and (D); and

(II) economic status;

(III) age intervals.

(F) PROHIBITIONS.—The Commissioner shall not include in the postsecondary student data system, data, or require the collection of such data, that—

(i) the Commissioner shall ensure secure, periodic data matches by entering into data
sharing agreements with each of the following Federal agencies and offices: 

"(I) The Secretary of the Treasury and the Commissioner of the Internal Revenue Service, in order to assess the use of postsecondary educational benefits and the outcomes of servicemembers.

"(II) The Secretary of Defense, in order to assess the use of postsecondary educational benefits and outcomes of veterans.

"(III) The Secretary of Veterans Affairs, in order to evaluate labor market outcomes of former postsecondary education students.


"(V) The Chief Operating Officer of the Office of Federal Student Aid, to analyze the use of postsecondary educational benefits provided under this Act.

"(VI) The Commissioner of the Social Security Administration, in order to evaluate employment, and further education, by program status, and repayment plan.


"(ii) The heads of Federal agencies and offices described under clause (i) shall enter into data sharing agreements with the Commissioner to ensure secure, periodic data matches as described in this paragraph.

"(B) CATEGORIZATION OF DATA.—The Commissioner shall, at a minimum, seek to ensure that the secure periodic data system matches described in subparagraph (A) permit consistent reporting of the following categories of data for all postsecondary students:

"(I) Enrollment, retention, transfer, and completion outcomes for all postsecondary students.

"(ii) Financial indicators for postsecondary students receiving Federal grants and loans, including grant and loan aid by source, cumulative student debt, loan repayment status, and repayment plan.

"(iii) Post-completion outcomes for all postsecondary students, including earnings, employment, and further education, by program of study and credential level and as measured—

"(I) immediately after leaving postsecondary education; and

"(II) at time intervals appropriate to the credential level and as earned.

"(C) PERIODIC DATA MATCH STREAMLINING AND CONFIDENTIALITY.—

"(I) STREAMLINING.—In carrying out the secure periodic system matches under this paragraph, the Commissioner shall—

"(I) ensure that such matches are not continuous, but occur only periodically at appropriate intervals, as determined by the Commissioner to meet the goals of subparagraph (A); and

"(II) seek to—

"(a) streamline the data collection and reporting requirements for institutions of higher education;

"(bb) minimize duplicative reporting across or within Federal agencies or departments, including reporting requirements applicable to institutions of higher education under the Workforce Innovation and Opportunity Act (29 U.S.C. 3101 et seq.) and the Carl D. Perkins Career and Technical Education Act of 2006; and

"(cc) protect student privacy; and

"(dd) remove any application process for student loan benefit programs available to borrowers based on data available from different Federal data systems.

"(II) Except as required once every 3 years after the establishment of the postsecondary student data system under this subsection, the Commissioner, in consultation with the Advisory Committee, shall review methods for streamlining data collection from institutions of higher education and Federal agencies and programs within the Department and across Federal agencies that provide data for the postsecondary student data system.

"(III) The Commissioner shall ensure that any periodic matching or sharing of data through periodic data system matches established in accordance with this paragraph—

"(I) complies with the security and privacy protections described in paragraph (1)(C)(iv) and other Federal data protection protocols;

"(II) follows best practices commensurate with the sensitivity of specific data elements or metrics;

"(III) does not result in the creation of a single standing, linked Federal database at the Department that maintains the information reported across other Federal agencies; and

"(IV) discloses to postsecondary students what data are included in the data system and periodically matched and how the data are used.

"(IV) CORRECTION.—The Commissioner, in consultation with the Advisory Committee, shall establish a process for students to request access to only their personal information for inspection and request corrections to inaccurate information that protects the student’s personally identifiable information. The Commissioner shall respond in writing to every request for a correction from a student.

"(V) IN GENERAL.—The Commissioner shall make the summary aggregate information described in subparagraph (C), at a minimum, publicly available through a user-friendly consumer information website and an analytic tool that—

"(I) provides appropriate mechanisms for users to customize and filter information by institutional and student characteristics;

"(II) allows users to build summary aggregate reports of information, including reports that allow comparisons across multiple institutions and programs, subject to subparagraph (B);

"(III) uses appropriate statistical disclosure limitation techniques necessary to ensure that the data released to the public cannot be used to identify specific individuals; and

"(IV) provides users with appropriate contextual factors to make comparisons, which may include national median figures of the summary aggregate information described in subparagraph (C).

"(B) NO PERSONALLY IDENTIFIABLE INFORMATION.—The summary aggregate information described in this paragraph shall not include personally identifiable information.

"(C) SUMMARY AGGREGATE INFORMATION AVAILABLE.—The summary aggregate information described in this paragraph shall, at a minimum, include each of the following for each institution of higher education:

"(I) Measures of student access, including—

"(I) admissions selectivity and yield; and

"(II) enrollment, disaggregated by each category described in paragraph (2)(C)(ii).

"(II) Measures of student progression, including retention rates and persistence rates, disaggregated by each category described in paragraph (2)(C)(ii).

"(III) Measures of student completion, including—

"(I) transfer rates and completion rates, disaggregated by each category described in paragraph (2)(C)(ii); and

"(II) number of completions, disaggregated by each category described in paragraph (2)(C)(ii).

"(IV) Measures of student costs, including—

"(I) tuition, required fees, total cost of attendance, and net price after total grant aid, disaggregated by in-State tuition or in-State institutional status (if applicable), and credential level; and

"(II) typical grant amounts and loan amounts received by students reported separately from Federal, State, local, and institutional sources, and cumulative debt, disaggregated by each category described in paragraph (2)(C)(ii) and completion status.

"(V) Measures of postcollege student outcomes, including employment rates, mean and median earnings, loan repayment and default rates, and further education rates. These measures shall—

"(I) be disaggregated by each category described in paragraph (2)(C)(ii) and completion status; and

"(II) be measured immediately after leaving postsecondary education and at time intervals appropriate to the credential sought or earned.

"(D) DEVELOPMENT CRITERIA.—In developing the method and format of making the information described in paragraph (1)(C)(i) publicly available, the Commissioner shall—

"(I) focus on the needs of the users of the information, which will include students, parents, student loan professionals, researchers, and other consumers of education data;

"(II) take into consideration, to the extent practicable, the guidelines described in paragraph (1)(C)(i), and relevant successor documents or recommendations of such guidelines;

"(iii) use modern, relevant technology and enhance and update the postsecondary student data system with information, as necessary to carry out the purpose of this paragraph;

"(iv) ensure data privacy and security in accordance with standards and guidelines developed by the National Institute of Standards and Technology, and in accordance with any other Federal law relating to privacy or security, including complying with the requirements of subsections (d) and (e) of title 44, United States Code, specifying security categorization under the Federal Information Processing Standards, requirements, and setting of National Institute of Standards and Technology security baseline controls at the appropriate level; and

"(v) conduct consumer testing to determine how to make the information as meaningful to users as possible.

"(D) PERMISSIBLE DISCLOSURES OF DATA.—

"(A) DATA REPORTS AND QUERIES.—

"(I) IN GENERAL.—Not later than 4 years after the date of enactment of the College Transparency Act, the Commissioner shall develop and implement a secure process for making student-level, non-personally identifiable information, with direct identifiers removed, from the postsecondary student data system available for vetted research and evaluation purposes approved by the Commissioner in a manner compatible with practices for disclosing National Center for Education Statistics restricted-use survey data as in effect on the day before the date of enactment of the College Transparency Act, or implementing any other reasonable administrative or publication restrictions to ensure data privacy and security. Such process shall be approved by the National Center for Education Statistics' Disclosure Review Board.

"(II) PROVIDING DATA REPORTS AND QUERIES TO INSTITUTIONS AND STATES.
“(I) IN GENERAL.—The Commissioner shall provide feedback reports, at least annually, to each institution of higher education, each postsecondary education system that fully participates in a postsecondary education data system, and each State higher education body as designated by the governor.

(II) FEEDBACK REPORTS.—The feedback reports under this clause shall include program-level and institution-level information from the postsecondary student data system regarding students who are associated with institutional or, for State representatives, the institutions within that State, on or before the date of the report, on measured student performance and workforce outcomes, provided that the feedback aggregate summary reports protect the privacy of individuals.

(iii) LIMITATION OF USE FOR FEDERAL AGENCIES.—The Commissioner shall, in consultation with the Advisory Committee and as soon as practicable, create a process through which States, institutions of higher education, and students in each State may submit lists of secondary school students enrolled in that State, which the Commissioner shall include in the postsecondary student data system.

(iv) REGULATIONS.—The Commissioner shall promulgate regulations to ensure, to the extent possible, that data collected under this subsection, including the aggregate outcomes for those students who enrolled at an institution of higher education, are aggregated to the greatest extent possible, and that the data protect the privacy of individuals and that the State data submitted to the Commissioner, as the Commissioner may request to carry out the purposes of this Act.

(v) DISCLOSURE LIMITATIONS.—In carrying out the training and technical assistance to States, the Commissioner shall ensure that the data released to the public cannot include personally identifiable information or be used to identify specific individuals.

(vi) SACK OF DATA PROHIBITED.—Data collected under this subsection, including the public-use data set and data comprising the summary aggregate information available under this subsection, shall not be sold to any third party by the Commissioner, including any institution of higher education or any other entity.

(vii) LIMITATION ON USE BY OTHER FEDERAL AGENCIES.—

(I) IN GENERAL.—The Commissioner shall not provide any additional Federal agency to use data collected under this subsection for any purpose except—

(I) for vetted research and evaluation conducted by the Federal agency, as described in subparagraph (A)(i); or

(II) for a purpose explicitly authorized by this Act.

(II) PROHIBITION ON LIMITATION OF SERVICES.—The Secretary, or the head of any other Federal agency, shall not use data collected under this subsection to limit services to students.

(viii) LAW ENFORCEMENT.—Personally identifiable information collected under this subsection shall not be used by the Secretary or any Federal entity to establish any Federal ranking system of institutions of higher education or a system that results in a summative Federal rating of institutions of higher education.

(ix) PROHIBITION ON USE.—Nothing in this paragraph shall be construed to prevent the use of individual categories of aggregate information to be used for accountability purposes.

(x) RULE OF CONSTRUCTION REGARDING COMMERCIAL USE OF DATA.—Nothing in this paragraph shall be construed to prohibit third parties from publicly releasing available information in this data system for commercial use.

(xi) SUBMISSION OF DATA.—

(1) REQUIRED SUBMISSION.—Each institution of higher education participating in a program under title IV, or the assigned agent of such institution, shall, for each eligible program, in accordance with section 487(a)(17), collect, and submit to the Commissioner, the data requested by the Commissioner to carry out this subsection.

(2) VOLUNTARY SUBMISSION.—Any institution of higher education not participating in a program under title IV may voluntarily participate and submit data to the Commissioner, as the Commissioner may request to carry out the purposes of this Act.

(3) FAILURE TO REPORT.—In the event that an eligible program is not maintained by an institution of higher education not participating in the program, the Commissioner may request that the institution of higher education notify the Commissioner, in a timely manner and to the satisfaction of the Secretary.

(4) USE OF DATA.—The Commissioner shall include—

(A) data collected by the Commissioner under paragraph (3) in the Integrated Postsecondary Education Data System (IPEDS), or any other Federal institution of higher education data collection effort (as designated by the Secretary), in a timely manner and to the satisfaction of the Secretary.

(b) REPEAL OF PROHIBITION ON STUDENT DATA SYSTEM.—Section 134 of the Higher Education Act of 1965 (20 U.S.C. 1019c) is repealed.

(c) INSTITUTIONAL REQUIREMENTS.—

(1) IN GENERAL.—(Par. 17) of section 487(a) of the Higher Education Act of 1965 (20 U.S.C. 1019a) is amended to read as follows:

(2) EFFECTIVE DATE.—The amendment made by paragraph (17) shall take effect on the date that is 4 years after the date of enactment of this Act.

(d) TRANSITION PROVISIONS.—The Secretary of Education and the Commissioner for Education Statistics shall take such steps as are necessary to ensure that the development and maintenance of the postsecondary student data system required under section 132(i) of the Higher Education Act of 1965, as added by subsection (b) of this section, occurs in a manner that reduces the reporting burden on entities that report to the Integrated Postsecondary Education Data System (IPEDS).

SA 4799. Mr. PETERS (for himself, Mr. PORTMAN, Mr. WARNER, Ms. COLLINS, Mr. KING, Mr. RUBIO, Mr. RISCH, Ms. ROSEN, Mr. CORNYN, and Mr. BURR) submitted an amendment intended to be proposed to amendment SA 1367 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 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, add the following:

DIVISION E—FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2021

SEC. 5101. SHORT TITLE.

This division may be cited as the “Federal Information Security Modernization Act of 2021.”

SEC. 5102. DEFINITIONS.

In this division, unless otherwise specified:
(1) ADDITIONAL CYBERSECURITY PROCE-
dURE.—The term ‘‘additional cybersecurity procedure’’ has the meaning given the term in section 3552(b) of title 44, United States Code.

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

(3) APPROPRIATE CONGRESSIONAL COMMIT-
tees.—The term ‘‘appropriate congressional committees’’ means—
(A) the Committee on Homeland Security and Governmental Affairs of the Senate;
(B) the Committee on Oversight and Reform of the House of Representatives; and
(C) the Committee on Homeland Security of the House of Representatives.

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

(5) INCIDENT.—The term ‘‘incident’’ has the meaning given the term in section 3522(b) of title 44, United States Code.

(6) NATIONAL SECURITY SYSTEM.—The term ‘‘national security system’’ has the meaning given the term in section 3522(b) of title 44, United States Code.

(7) PENETRATION TEST.—The term ‘‘penetra-
tion test’’ has the meaning given the term in section 3522(b) of title 44, United States Code, as amended by this division.

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

TITLE LI—UPDATES TO FISMA

SEC. 5121. TITLE 44 AMENDMENTS. (a) SUBCHAPTER I AMENDMENTS.—Sub-
chapter I of chapter 35 of title 44, United States Code, is amended—
(1) in section 3504—
(A) in subsection (a)(1)(B)—
(i) by striking clause (v) and inserting the following:
‘‘(v) confidentiality, privacy, disclosure, and sharing of information;’’;
(ii) by redesigning clause (vi) as clause (vii); and
(iii) by inserting after clause (v) the fol-
lowing:
‘‘(vii) in consultation with the National Cyber Director and the Director of the Cy-
bersecurity and Infrastructure Security Agency, the information system, or a component of an information system; and

(2) in section 3505—
(A) in paragraph (3) of the first subsection designated as subsection (c)—
(i) in subparagraph (B)—
(I) inserting ‘‘the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, and ‘the Comptroller General’’; and
(ii) by striking at the end;
(ii) 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; and

(B) in subsection (b)(3), by inserting ‘‘security, after ‘efficiency,’;’’ and

(4) in section 3513—
(A) by redesignating subsection (c) as subsection (d); and
(B) by inserting after subsection (b) the following:
‘‘(c) Each agency providing a written plan under subsection (b) shall provide any portion of the written plan addressing informa-
tion security to the Director of the Cybersecurity and Infrastructure Security Agency.’’;

(b) SUBCHAPTER II DEFINITIONS.—
(1) IN GENERAL.—Section 3522(b) of title 44, United States Code, is amended by striking paragraphs (1), (2), (3), (4), (5), (6), (7), and (11), respectively; and
(B) by inserting after paragraph (2), as so redesignated, the following:
‘‘(1) The term ‘‘additional cybersecurity procedure’’ means a process, procedure, or other activity that is established in excess of the information security standards promul-
gated under section 11313(b) of title 40 to in-
crease the security and reduce the cyberse-
curity risk of agency systems.’’;

(C) by inserting after paragraph (6), as so redesignated, the following:
‘‘(7) The term ‘‘high value asset’’ means infor-
mation or a information system that the head of an agency determines so critical to the agen-
cy that the loss or corruption of the information or a information system would have a serious impact on the ability of the agency to perform the mission of the agency or conduct business.’’;

(2) in section 3513—
(A) in paragraph (4), by striking ‘‘diagnose
and improve’’ and inserting ‘‘integrate, de-
liver, diagnose, and improve’’;

(3) in section 3522—
(A) by striking the section heading and in-
serting ‘‘section 3522(b)’’.

III. IN GENERAL.—The term ‘‘security risk of agency systems.’’;

IV. CONFORMING AMENDMENTS.—
(A) HOMELAND SECURITY ACT OF 2002.—Sec-
tion 103(a) of the Homeland Security Act of 2002 (6 U.S.C. 511(1)(A)) is amended by striking ‘‘section 3552(b)(5)’’ and inserting ‘‘section 3552(b);’’

(B) TITLES.—
(I) SECTION 2222.—Section 2222(b)(8) of title 10, United States Code, is amended by striking ‘‘section 3522(b)(6)’’ and inserting ‘‘section 3522(b);’’

(ii) the last; and

(c) SUBCHAPTER II AMENDMENTS.—Sub-
chapter II of chapter 33 of title 44, United States Code, is amended—
(1) in section 3551—
(A) in paragraph (4), by striking ‘‘diagnose
and improve’’ and inserting ‘‘integrate, de-
liver, diagnose, and improve’’;

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

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

(D) by adding at the end the following:
‘‘(7) recognize that each agency has spe-
cific mission requirements and, at times, specific mission 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 ex-
pected to have the capability to secure the systems of the agency from advanced adver-
saries alone; and

(9) recognize that a holistic Federal cy-
bersecurity model is necessary to account for differences between the missions and ca-
pabilities of agencies.’’;

(2) in section 3553—
(A) by striking the section heading and in-
serting ‘‘Authority and functions of the Di-
rector and the Director of the Cybersecurity and Infrastructure Security Agency’’;

(B) in subsection (a)—
(i) in paragraph (1), by inserting ‘‘, in con-
sultation with the Director of the Cybersecu-
ry and Infrastructure Security Agency and the National Cyber Director,” before ‘‘over-
seeing’’;

(ii) in paragraph (4), by striking ‘‘and’’ at the end; and

(iii) by adding at the end the following:
‘‘(8) promoting, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, the National Institute of Standards and Tech-
ology—
“(A) the use of automation to improve Federal cybersecurity and visibility with respect to the implementation of Federal cybersecurity; and

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

“(C) in subsection (i) by striking the subsection heading and inserting “CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY”;

“(ii) upon preceding paragraph (1), by striking “The Secretary, in consultation with the Director” and inserting “The Director of the Cybersecurity and Infrastructure Security Agency,” in consultation with the Director and the National Cyber Director;”;

“(ii) in paragraph (2)—

(I) in subparagraph (A), by inserting “and” and reporting requirements under subchapter IV of this title” after “section 3556”; and

(II) in subparagraph (D), by striking “and” at the end; and

“(iii) by inserting at the end the following:

“(3) in section 3554—

(A) in subsection (a)—

(I) in paragraph (1)—

(i) by striking “and” at the end;

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

“(K) by inserting after subsection (h) the following:

“(III) the National Cyber Director;

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

“(B) the trends identified in the Federal risk assessment performed under subsection (i);”;

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

“(A) the use of automation to improve Federal cybersecurity; and

(3) in section 3554—

(A) in subsection (a)—

(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:

“(4) evaluation of vulnerability disclosure practices performed by the Department of Homeland Security under section 3553(b)(9);”;

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

“(II) the results of vulnerability disclosure 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, including information that is reported by, or under the supervision of, the agency, on a periodic basis, as determined by the head of the agency.”;

“(B) in clause (i) by inserting “in accordance with standards” and inserting “in accordance with—”;

(II) in subparagraph (B)—

(aa) by striking “in accordance with standards” and inserting “in accordance with—”;

(bb) by inserting at the end the following:

“(ii) the vulnerability disclosure program described in paragraph (1)(G);”;

(III) 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)—

(I) in subparagraph (A)—

(aa) in clause (ii), by striking “and” at the end;

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

(cc) by adding at the end the following:

“(y) ensure that—

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

(W) senior agency information security officers of component agencies report to—
“(aa) the senior information security officer of the agency or an equivalent official; and

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

and

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

(B) in subsection (b)—

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

“(1) pursuant to subsection (a)(1)(A), performing ongoing and continuous agency system risk assessment, which may include using guidelines and automated tools consistent with standards and guidelines promulgated under section 11313 of title 40, as applicable;”;

(ii) in paragraph (2)—

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

“(B) in subsection (a)(1)(A), performing ongoing and continuous agency system risk assessment, which may include using guidelines and automated tools consistent with standards and guidelines promulgated under section 11313 of title 40, as applicable;”;

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

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

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

“(B) evaluates the adequacy and effectiveness of information security policies, procedures, and practices of the agency to address the risks identified in the agency system risk assessment performed under subsection (a)(1)(A), including an analysis of the agency’s cybersecurity and incident response capabilities using the metrics established under section 2240 of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c));

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

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

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

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

“(B) may include a classified annex.

“(C) Any information that the head of an agency shall ensure that, to the greatest extent practicable, and if classified, to the greatest extent practicable, in an unclassified and otherwise uncontrolled form; and

“(B) may include a classified annex.

“(C) Any information that the head of an agency shall ensure that, to the greatest extent practicable, and classified, to the greatest extent practicable, in an unclassified and otherwise uncontrolled form; and

“(B) may include a classified annex.

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

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

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

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

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

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.
VerDate Sep 11 2014 06:22 Nov 19, 2021 Jkt 029060 PO 00000 Frm 00067 Fmt 0624 Sfmt 0634 E:\CR\FM\A18NO6.057 S18NOPT1ctelli on DSK11ZRN23PROD with SENATE

(1) TABLE OF SECTIONS.—The table of sections for chapter 35 of title 44, United States Code, is amended—

(A) by striking the item relating to section 3555 and inserting the following: ‘‘3555. Authority and functions of the Director and the Secretary for the Cyberspace and Infrastructure Security Agency’’; and

(B) 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 ‘‘annual’’ and inserting ‘‘thereafter’’; 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) from ‘‘the report required under section 3553(c) of title 44, United States Code’’ and inserting ‘‘that report’’.

(3) NIST RESPONSIBILITIES.—Section 204(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) INCORPORATION.—Chapter 35 of title 44, United States Code, is amended by adding at the end the following:

‘‘SUBCHAPTER IV—FEDERAL SYSTEM OCCURRED INCIDENT RESPONSE’’

4351. Definitions

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

(b) 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 Oversight and Reform Committee of the House of Representatives;

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

(F) the appropriate agency, commission, or appropriations committee of Congress;

(G) the Director;

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

(I) the National Cyber Director; and

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

(K) the inspector general of any impacted agency.

(2) AWAREDEE.—The term ‘‘awaredee’’—

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

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

(3) BREACH.—The term ‘‘breach’’ means—

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

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

(4) CONTRACTOR.—The term ‘‘contractor’’ means—

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

(B) any person or business that collects or maintains information, including personally identifiable information, on behalf of an agency.

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

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

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

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

(9) VULNERABILITY DISCLOSURE.—The term ‘‘vulnerability disclosure’’ means a vulnerability identified under section 3559b.

3552. Reports

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

(1) determine whether notice to any individual potentially affected by the breach is appropriate based on an assessment of the risk of harm to the individual that considered—

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

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

(C) the type of breach; and

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

(2) as appropriate, provide written notice to each individual potentially affected by the breach:

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

(B) through an appropriate alternative method; or

(C) through an appropriate alternative method determined by the head of the agency or a designated senior-level individual of the agency selects based on factors determined by the Director.

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

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

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

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

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

(B) may include a telephone number or a website;

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

(5) any applicable educational materials relating to what individuals can do in response to a breach that potentially affected by breaches that are not determined to be major incidents; or

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

(c) DELAY OF NOTIFICATION.—

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

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

(B) reveal sensitive sources and methods;

(C) cause damage to national security; or

(D) hamper security remediation actions.

(2) DOCUMENTATION.—The Director, the Attorney General, or the National Director of Intelligence, the Secretary of Homeland Security, the Director of the Cybersecurity and Infrastructure Security Agency, and the head of the agency and the inspector general of the agency that experienced the breach.

(3) CONTENTS.—A report required under paragraph (a) shall include a written statement from the Director, the Attorney General, or the National Director of Intelligence, the Secretary of Homeland Security, the Director of the Cybersecurity and Infrastructure Security Agency, and the head of the agency and the inspector general of the agency that experienced the breach.

(4) UPDATE NOTIFICATION.—If an agency determines there is a significant change in the reasonable basis to continue that a breach occurred, a significant change to the determination made under subsection (a)(1), or that it is necessary to update the details of the information provided to impacted individuals as described in paragraph (a)(2), the agency shall as expeditiously as practicable and without unreasonable delay, and in any case not later than 30 days after such a determination, notify each individual who received a notification pursuant to subsection (a) of those changes.

(5) EXEMPTION FROM NOTIFICATION.—

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

(A) encrypted; and

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

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

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

(B) the Attorney General.

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

4353. Audit

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

(1) the Director from issuing guidance relating to notifications or the head of an agency from notifying individuals potentially affected by breaches that are not determined to be major incidents; or
“(2) the Director from issuing guidance relating to notifications of major incidents or the head of an agency from providing more information than described in subsection (b) when an agency individually potentially affected by breaches.

§3593. Congressional and Executive Branch reports

(1) INITIAL REPORT.—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 notify the appropriate reporting entities a written report and, to the extent practicable, provide a briefing to the Committee on Homeland Security and Governmental Affairs, the Senate, and the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, and the appropriate authorization and appropriations committees of Congress, taking into account—

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

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

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

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

(A) a summary of the information available as of the major incident, including how the major incident occurred, information indicating that the major incident may be a breach, and information relating to the major incident as a breach, based on information available to agency officials as of the date on which the agency submits the report;

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

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

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

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

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

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

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

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

(6) an update to the assessment of the risk to agency operations, or to impacts on other agency or non-Federal entity operations, affected by the major incident based on information available to agency officials as of the date on which the agency provides the update; and

(7) the detection, response, and remediation actions of the agency, including any support provided by the Cybersecurity and Infrastructure Security Agency under section 359(d) and status updates on the notification process described in section 3592, including any delay or exemption described in subsection (c) or (e), respectively, of section 3592, if applicable.

(c) UPDATE REPORT.—If the agency determines that there is any significant change in the understanding of the agency of the scope, scale, or consequence of a major incident for which an agency submitted a written report under subsection (a), the agency shall provide an updated report to the appropriate reporting entities and, to the extent permitted by applicable law, including privacy and statutory laws—

(A) a summary of the information available as of the major incident, including how the major incident occurred, information indicating that the major incident may be a breach, and information relating to the major incident as a breach, based on information available to agency officials as of the date on which the agency submits the report;

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

(C) an update to the information and any information sharing limitations and protections, such as limitations and protections relating to law enforcement, national security, privacy, statistical confidentiality, or other factors determined by the Director.

(d) ANNUAL REPORT.—Each agency shall submit as part of the annual report required under section 3595(c)(1) of this title a description of each major incident that occurred during the 1-year period preceding the date on which the annual report is submitted.

(e) DELAY AND EXEMPTION REPORT.—

(1) IN GENERAL.—The Director shall submit to the appropriate notification entities a written report—

(A) a summary of the information available as of the major incident, including how the major incident occurred, information indicating that the major incident may be a breach, and information relating to the major incident as a breach, based on information available to agency officials as of the date on which the agency submits the report; and

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

(2) COMPONENTS.—The Director may include—

(A) a summary of the information available as of the major incident, including how the major incident occurred, information indicating that the major incident may be a breach, and information relating to the major incident as a breach, based on information available to agency officials as of the date on which the agency submits the report;

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

(C) an update to the information and any information sharing limitations and protections, such as limitations and protections relating to law enforcement, national security, privacy, statistical confidentiality, or other factors determined by the Director.

(2) CONGRESS FROM REQUESTING ADDITIONAL INFORMATION.—The Director may include a classified component.

(f) TREATMENs BRIEFING.—

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

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

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

(B) may include a classified component.

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

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

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

§3594. Government information sharing and incident response

(a) IN GENERAL.—

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

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

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

(B) include a written report submitted under section 3597(b).
(2) PROCEDURES.—

(A) MAJOR INCIDENT.—Following a report of a breach or major incident by a contractor or awardee under paragraph (1), the agency, in consultation with the contractor or awardee, shall carry out the requirements under sections 3592, 3593, and 3594 with respect to the major incident.

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

§3596. Training

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

(b) REQUIREMENTS.—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 an incident to the agency if identified as a covered incident involving information in any medium or form, including paper, oral, and electronic.

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

§3597. Analysis and report on Federal incidents

(a) ANALYSIS OF FEDERAL INCIDENTS.—

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

(A) the causes of incidents, including—

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

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

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

(C) cross-Federal Government root causes of incidents at agencies;

(D) agency incident response, recovery, and remediation actions and the effectiveness of the applicable agencies.

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

(F) Federal Government cybersecurity and incident response capabilities using the metrics established under subsection (b) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c));

(2) AUTOMATED ANALYSIS.—The analyses developed under paragraph (1) shall, to the extent that the submissions are applicable, be machine readable data, automation, and machine learning processes.

(3) SHARING OF DATA AND ANALYSIS.—

(A) IN GENERAL.—The Director shall share the analyses—

(i) in human-readable written products; and

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

(B) ANNUAL REPORT ON FEDERAL INCIDENTS.—Not later than 2 years after the date of enactment of this section, and not less frequently than annually thereafter, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director and other Federal agencies as appropriate, shall submit to the appropriate notification entity that includes—

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

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

(C) an analysis of the agency’s performance against the metrics established under subsection (b)(1)(A) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c)).

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

(d) INFORMATION PROVIDED BY AGENCIES.—

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

(2) NONCOMPLIANCE REPORTS.—

(A) IN GENERAL.—Subject to subparagraph (B), during any year during which the head of an agency does not provide data for an incident the head of the Cybersecurity and Infrastructure Security Agency shall sufficiently compile information such that no specific incident of an agency can be identified, except with the concurrence of the Director of the Office of Management and Budget and in consultation with the appropriate committees of Congress.

(B) REQUIREMENTS.—The head of the agency or the committee having jurisdiction over the agency shall submit to the appropriate reporting entity a report that in—

(i) a specific analysis of breaches; and

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

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

(C) cross-Federal Government root causes of incidents at agencies;

(D) agency incident response, recovery, and remediation actions and the effectiveness of the applicable agencies.

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

(F) Federal Government 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));

(2) AUTOMATED ANALYSIS.—The analyses developed under paragraph (1) shall, to the extent that the submissions are applicable, be machine readable data, automation, and machine learning processes.

(3) SHARING OF DATA AND ANALYSIS.—

(A) IN GENERAL.—The Director shall share the analyses—

(i) in human-readable written products; and

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

(B) ANNUAL REPORT ON FEDERAL INCIDENTS.—Not later than 2 years after the date of enactment of this section, and not less frequently than annually thereafter, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director and other Federal agencies as appropriate, shall submit to the appropriate notification entity that includes—

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

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

(C) an analysis of the agency’s performance against the metrics established under subsection (b)(1)(A) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c)).

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

(d) INFORMATION PROVIDED BY AGENCIES.—

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

(2) NONCOMPLIANCE REPORTS.—

(A) IN GENERAL.—Subject to subparagraph (B), during any year during which the head of an agency does not provide data for an incident the head of the Cybersecurity and Infrastructure Security Agency shall sufficiently compile information such that no specific incident of an agency can be identified, except with the concurrence of the Director of the Office of Management and Budget and in consultation with the appropriate committees of Congress.

(B) REQUIREMENTS.—The head of the agency or the committee having jurisdiction over the agency shall submit to the appropriate reporting entity a report that in—

(i) a specific analysis of breaches; and

(ii) system vulnerabilities, including zero days, unpatched systems, and information system configuration deficiencies;
“(2) stipulate that the National Cyber Dier-
rector shall declare a major incident at each agency impacted by an incident if the Direc-
tor of the Cybersecurity and Infrastructure Security Agency determines that an inci-
dent—

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

(B) is enabled by—

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

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

(3) stipulate that, in determining whether an incident constitutes a major incident be-
cause that incident—

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

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

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

(i) the Privacy and Civil Liberties Over-
sight Board; and

(ii) the Chair of the Federal Trade Com-
mission.

(c) SIGNIFICANT NUMBER OF INDIVIDUALS.— In determining what constitutes a signif-
ciant number of individuals, the Chief Information Officer shall—

(1) determine a threshold for a min-
umimum number of individuals that constitutes a significant amount; and

(2) may not determine a threshold de-
scribed in paragraph (1) that exceeds 5,000 in-
dividuals.

(d) EVALUATION AND UPDATES.—Not later than 2 years after the date of enactment of the Federal Information Security Modernization Act of 2020, or not less frequently than every 2 years thereafter, the Director shall submit to the Committee on Homeland Secu-
ritv and Government Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives an evalua-
tion, which shall include—

(1) an update, if necessary, to the guid-
ance issued under subsection (a); and

(2) the definition of the term "major inci-
dent" included in the guidance issued under subsection (a); and

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

(2) CHERICAL AMENDMENT.—The table of sections for chapter 3 of title 44, United States Code, is amended by adding at the end the following:

"SUBCHAPTER L—SUBCHAPTER L of subtitle III of title 44, United States Code, is amended—"

"(2) in subsection (b), by striking "including security best practices" after "managing the"; and

(5) in subsection (b)(1), in the paragraph heading, by striking "CIOS" and inserting "chief Information Officers"; and in subsection (b)(2), by striking "information sharing and incident response."; and

(5) in subsection (c), by adding at the end the following:

"(6) by striking "including security best practices" after "managing the"

"SEC. 5122. AMENDMENTS TO SUBTITLE III OF TITLE 40.

(a) MODERNIZING GOVERNMENT TECH-

(1) in section 1330(a)—

(A) by striking paragraph (5)(A), by inserting "im-
proving the cybersecurity of systems and" before "cost savings activities"; and

(B) in paragraph (7)—

(i) in the paragraph heading, by striking "‘ciso’ and inserting "CIO’; (ii) by striking "in evaluating projects" and inserting "in assessing the following:

(A) CONSIDERATION OF GUIDANCE.—In eval-
uating projects;

(B) CONSULTATION.—In using funds under para-
graph (1), the Cybersecurity and Infrastructure Security Agency and the National Cyber Director, as appropriate; and

(2) in section 1378—

(A) by striking section (a)(1) and inserting the following:

(i) in clause (i), by striking "by the end at the following:

(B) PROPOSAL EVALUATION.—The Director shall:

(A) give consideration for the use of amounts in the Fund to improve the security of high value assets; and

(B) require that any proposal for the use of amounts in the Fund includes a cybersecurity plan, including a supply chain risk man-
age ment plan, to be reviewed by the member of the Technology Modernization Board de-
scribed in subsection (c); and

(C) in subsection (c)—

(i) in paragraph (2)(A), by inserting "includ-
ing a consideration of the impact on high value assets" after "operational risks";

(ii) in paragraph (5)—

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

(II) in subparagraph (B), by striking the pe-
riod at the end and inserting "and"; and

(III) by adding at the end the following:

(O) a senior official from the Cybersecu-
ritv and Infrastructure Security Agency of the Department of Homeland Security, ap-
pointed by the Director; and

(iii) in paragraph (6)(A), by striking "shall be-
" and all that follows through "employees";

(C) in section 1372(b)—

(ii) by striking "shall include" and inserting "shall be 4 employ-
employees";

(D) in section 1373(d)—

(ii) specifically denote cybersecurity

(E) in section 1374(a)—

(i) in paragraph (3)—

(aa) by striking "including data" and in-
serting "including which shall—

(1) include "(b) in clause (i), as so designated, by striking "", and performance" and inserting "security, and performance; and"; and

(bb) in paragraph (A), by striking "(I)" and inserting "(I) and (II)".

(2) in subsection (c), by striking "in the anal-
ysis of the" and inserting "in the analysis of the following:

(i) the need to employ standards for cost-effec-
tive, risk-based information security for all systems, operations, and assets within or under the supervision of the agency that are managed by the agency, including that promul-
gated by the Director under this section, if such standards contain, at a minimum, the

"(iii) The Director shall provide to the Na-
tional Cyber Director any cybersecurity

"(iv) may not determine a threshold for a min-
umimum number of individuals that constitutes a significant amount; and

(1) the definition of the term 'major inci-
dent' included in the guidance issued under subsection (a); and

(2) in paragraph (1)(A), by inserting "includ-
ing a consideration of the impact on high value assets" after "operational risks"; and

(B) requires that any proposal for the use of amounts in the Fund includes a cybersecurity plan, including a supply chain risk management plan, to be reviewed by the member of the Technology Modernization Board described in subsection (c); and

(C) in subsection (c)—

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

(II) in paragraph (5)—

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

(II) in subparagraph (B), by striking the pe-
riod at the end and inserting "and"; and

(III) by adding at the end the following:

(O) a senior official from the Cybersecu-
ritv and Infrastructure Security Agency of the Department of Homeland Security, ap-
pointed by the Director; and

(2) the head of the component agency; and

(4) in section 1317, by inserting "secu-
ritv," before "or schedule"; and

(5) in section 1319(b)(1), in the paragraph heading, by striking "CIOS" and inserting "Chief Information Officers"; and

(d) SUBCHAPTER III.—Section 1311 of title 40, United States Code, is amended—

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

(2) in subsection (b)(1)(A), by striking "the Secretary of Homeland Infrastructure and Security" and insert-
ing "the Director of the Cybersecurity and Infrastructure Security Agency";

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

"(c) APPLICATION OF MORE STRINGENT STANDARDS.—"

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

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

"(b) to the greatest extent practicable and if the Director determines that the standards described in subparagraph (A) are necessary, employ those standards.

"(2) EVALUATION OF MORE STRINGENT STANDARDS.—If the Director determines that more stringent standards under paragraph (1), the head of an agency shall consider available risk information, such as—

"(A) any assessment or report required under section 3559A of title 44; and

"(B) any information from the National Institute of Standards and Technology, the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)), the Federal Institute of Technology issues a proposed standard pursuant to paragraph (2) and section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 276g–3(a)), the Director of the National Institute of Standards and Technology shall consider developing and, if appropriate and practical, develop, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, specifications to enable the efficient development of—

"(I) aspects of a standard, a proposal, or an amendment to a proposal that is necessary to understand and analyze—

"(aa) common across the Federal Government; or

"(bb) have a Government-wide impact;

"(C) guidance or policy promulgated under this section that is currently in effect;

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

"(E) any other information determined relevant by the head of the agency;".

(4) in subsection (d)—

"(A) the status of cybersecurity remedial actions performed under section 355A of title 44; and

"(B) any guidance or policy which changes were determined appropriate by the Director, or policy promulgated by the Director in response to agency systems that is known to the agency;

"(C) incident information of the agency;

"(D) information from—

"(i) the executive committee performing under section 3559A of title 44; and

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

"(E) threat hunting results under section 514 of the Federal Information Security Modernization Act of 2021; and

"(F) the cost of implementation of the standards performed under subparagraph (A) of section 3553(i) of title 44.

"(2) UPDATED GUIDANCE.—Not later than 90 days after the date on which a review is completed under paragraph (1), the Director of the Office of Management and Budget shall issue updated guidance or policy to agencies determined appropriate by the Director, based on the analysis required under section 3597(a) of title 44, United States Code, as added by this division.

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

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

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

"(C) any other information determined relevant by the head of the agency;".

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

"(5) AUTOMATED STANDARD IMPLEMENTATION VERIFICATION.—When the Director of the National Institute of Standards and Technology issues a proposed standard pursuant to paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 276g–3(a)), the Director of the National Institute of Standards and Technology shall review the efficacy of the guidance and policy promulgated by the Director in response to agency systems that is known to the agency; and

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

"(C) any other information determined relevant by the head of the agency;".

"(6) RESPONSIBILITIES OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.—(A) RESPONSIBILITIES OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.—When the Director of the Office of Management and Budget makes a determination under paragraph (1), the Director shall provide to the Committee on Homeland Security, the Committee on the Budget, and the National Academy of Public Administration, a description of any challenges the Director anticipates encountering; and

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

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

"(ii) enable the efficient development of—

"(aa) common across the Federal Government; or

"(bb) have a Government-wide impact;

"(C) guidance or policy which changes were determined appropriate by the Director, or policy promulgated by the Director in response to agency systems that is known to the agency;

"(D) any information from the vulnerability disclosure program established under section 3559B of title 44; and

"(E) threat hunting results under section 514 of the Federal Information Security Modernization Act of 2021; and

"(F) the cost of implementation of the standards performed under subparagraph (A) of section 3553(i) of title 44.

"(3) GUIDANCE ON RESPONDING TO INFORMATION REQUESTS.—Not later than 1 year after the date of enactment of this Act, the Director shall provide to the appropriate congressional committees a briefing on—

"(I) the causes of incidents;

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

"(III) a root cause analysis of incidents that—

"(1) identifies the causes of an incident or policy is appropriate.

"(2) the effectiveness of those actions; and

"(B) updating the information of the Federal Government.

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

"(E) any other information determined relevant by the head of the agency;".

"(4) STANDARD GUIDANCE AND TEMPLATES.—Not later than 1 year after the date of enactment of this Act, the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, the Comptroller General of the United States, and the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security, the Cybersecurity and Infrastructure Security Agency, the National Academy of Public Administration, shall—

"(I) develop, in consultation with the Director of the National Institute of Standards and Technology, specifications to enable the efficient development of—

"(aa) common across the Federal Government; or

"(bb) have a Government-wide impact;

"(C) any other information determined relevant by the head of the agency;".

"(5) CONTRACTOR AND AWARENESS GUIDANCE.—(A) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Director, in coordination with the Secretary of Homeland Security, the Secretary of Defense, the Administrator of General Services, and the heads of other agencies determined appropriate by the Director, shall—

"(i) provide—

"(aa) common across the Federal Government; or

"(bb) have a Government-wide impact;

"(C) any other information determined relevant by the head of the agency;".

"(6) UPDATED BRIEFINGS.—Not less frequently than once every 2 years, the Director shall provide to the appropriate congressional committees an update on the guidance and templates developed under paragraphs (2) through (4).
(c) Update to the Privacy Act of 1974.—Section 525a(b) of title 5, United States Code (commonly known as the “Privacy Act of 1974”) is amended—

(1) in paragraph (1), by striking “or” at the end;

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

(3) in subsection (b), by striking the following: “’(b) to another agency in furtherance of a response to an incident as defined in section 5352 of title 44 and pursuant to the information sharing requirements under section 3549a(1)(A) of title 44 if the head of the requesting agency has made a written request to the agency that maintains the record specifying the particular portion desired and the activity for which the record is sought.’’;

SEC. 5142. ADDITIONAL GUIDANCE TO AGENCIES ON PSIAMA UPDATES.

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

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

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

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

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

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

(4) interpreting the definition of “high value asset” under section 3552 of title 44, United States Code, as amended by this division; and

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

SEC. 5125. AGENCY REQUIREMENTS TO NOTIFY PRIVATE SECTOR ENTITIES IN RESPONSE TO INCIDENTS.

(a) Definitions.—In this section:

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

(2) SENSITIVE INFORMATION.—The term “sensitive information” has the meaning given the term by the Director in guidance issued under subsection (b).

(b) Guidance on Notification of Reporting Entities.—Not later than 180 days after the date of enactment of this Act, the Director shall issue guidance requiring the head of each agency to notify a reporting entity of an incident that is likely to substantially affect—

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

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

TITLE LI—IMPROVING FEDERAL CYBERSECURITY

SEC. 5141. MOBILE SECURITY STANDARDS.

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

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

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

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

(1) a requirement, pursuant to section 3506(c) of title 44, United States Code, for every agency to maintain a continuous inventory of every—

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

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

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

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

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

SEC. 5142. DATA AND LOGGING RETENTION FOR INCIDENT RESPONSE.

(a) Recommendations.—Not later than 2 years after the date of enactment of this Act, and not later than 3 years thereafter, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Attorney General, shall submit to the Director recommendations on requirements for logging events on agency systems and retaining other relevant data within the systems and networks of an agency.

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

(1) the types of logs to be maintained;

(2) the time period to retain the logs and other relevant data;

(3) the time periods for agencies to enable recommended logging and security requirements;

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

(5) requirements to ensure that, upon request, in a manner that excludes or otherwise reasonably protects personally identifiable information, and to the extent permitted by applicable law (including privacy and statistical laws), agencies provide logs to—

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

(B) the Federal Bureau of Investigation to investigate potential criminal activity; and

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

(c) Guidance.—Not later than 90 days after receiving the recommendations submitted under subsection (a), the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the Attorney General, shall, as determined to be appropriate by the agency, promulgate 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.

SEC. 5143. CISA AGENCY ADVISORS.

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

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

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

(2) performing risk assessments of agency systems; and

(3) other Federal cybersecurity initiatives.

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

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

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

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

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

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

SEC. 5144. FEDERAL PENETRATION TESTING POLICY.

(a) In General.—Subchapter II of chapter 3 of title 44, United States Code, is amended by adding at the end the following:

“§ 3559A. Federal penetration testing

“(a) Definitions.—In this section:

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

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

“(b) Guidance.—

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

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

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

“(2) Penetration testing guidance.—The guidance issued under this section shall—

“(A) require agencies to use the rules of engagement and plans of engagement to perform penetration testing;

“(B) ensure that—

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

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

“(B) require agencies to provide the rules of engagement and plans of engagement to the Director and the Director of the Cybersecurity and Infrastructure Security Agency, without regard to the status of the entity that performs the penetration testing.

“(c) Agency plans and rules of engagement.—The agency operational plan and rules of engagement of an agency shall—

“(1) include—

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

“(2) require agencies to develop an agency operational plan and rules of engagement to meet the requirements under subsection (b).
“(B) coordinate with the Director of the Cybersecurity and Infrastructure Security Agency to ensure that penetration testing is being performed; 

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

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

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

(C) inappropriate access to data; 

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

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

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

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

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

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

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

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

(1) assess frequently than annually, inventory all Federal penetration testing assets; and 

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

(f) PRIORITIZATION OF PENETRATION TESTING RESOURCES.— 

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

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

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

(B) the Federal risk assessment performed under section 3553(1); 

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

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

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

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

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

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

(b) DEADLINE FOR GUIDANCE.—Not later than 180 days after the date of enactment of this Act, the Director shall issue guidance to include feedback to improve the cybersecurity of the agency; and 

(2) by redesignating paragraph (9) as paragraph (10); and 

(3) by inserting after paragraph (8) the following: 

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

SEC. 5145. ONGOING THREAT HUNTING PROGRAM. 

(a) THREAT HUNTING PROGRAM.— 

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

(2) PLAN.—Not later than 180 days after the date of enactment of this Act, the Director shall— 

(A) establish a process to assess the capability to offer penetration testing as a service to Federal and non-Federal entities; 

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

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

SEC. 5146. CODIFYING VULNERABILITY DISCLOSURE PROGRAMS. 

(a) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by adding after the item relating to section 3559 the following: 

“3559B. Federal vulnerability disclosure programs 

(a) DEFINITIONS.—In this section: 

(1) The term ‘reporter’ means a vulnerability disclosure made to an agency by a reporter. 

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

(3) RESPONSIBILITIES FOR OB M.— 

(1) LIMITATION ON LEGAL ACTION.—The Director, in consultation with the Attorney General, shall issue guidance to agencies to not recommend or pursue legal action against a reporter or an individual that collects a vulnerability disclosure, and make publicly available a vulnerability disclosure policy for the agency, which shall— 

(A) provide a non-exhaustive list of the scope of the systems of the agency included in the vulnerability disclosure policy,
“(ii) the type of information system testing that is authorized by the agency; and
“(iii) the type of information system testing that is not authorized by the agency; and
“(iv) a comprehensive policy of the agency for sensitive information;
“(B) with respect to a report to an agency, describe—
“(1) how the reporter should submit the report; and
“(2) 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;
“(D) be mature in scope, to cover all Federal information systems used or operated by that agency or on behalf of that agency.
“(S) IDENTIFIED VULNERABILITIES.—The head of each agency shall incorporate any vulnerabilities reported under paragraph (2) into the vulnerability management process of the agency in order to track and remediate the vulnerability.
“(e) PAPERWORK REDUCTION ACT EXEMPTION.—The requirements of subchapter I (commonly known as the ‘Paperwork Reduction Act’) shall apply to a vulnerability disclosure program established under this section.
“(f) CONGRESSIONAL REPORTING.—Not later than 90 days after the date of enactment of this Act, and annually thereafter for a 3-year period, the Director shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives a briefing on the status of the vulnerability disclosure policies under this section at agencies, including, with respect to the guidance issued under subsection (b)(3), an identification of the agencies that are compliant and not compliant.
“(g) EXEMPTIONS.—The authorities and functions of the Director and Director of the Cybersecurity and Infrastructure Security Agency under this section shall not apply to national security systems.
“(h) DELEGATION OF AUTHORITY FOR CERTAIN ACTIVITIES.—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 3555(e)(2); and
“(2) to the Director of National Intelligence in the case of systems described in section 3555(e)(3).
“(i) CLERICAL AMENDMENT.—The table of sections for chapter 35 of title 44, United States Code, is amended by adding after the item relating to section 3559A, as added by section 204, the following:
“(3559B. Federal vulnerability disclosure programs.)

SEC. 5147. IMPLEMENTING PRESCRIPTION OF COMPROMISE AND LEAST PRIVILEGE PRINCIPLES.

(a) GUIDANCE.—Not later than 1 year after the date of enactment of this Act, the Director shall provide an update to the appropriate congressional committees on progress in increasing the internal defenses of agency systems, including—
“(1) shifting away from ‘trusted networks’ to implement security controls based on a presumption of compromise;
“(2) the implementation of least privilege principles in administering information security programs;
“(3) limiting the ability of entities that cause guidance to move laterally through or between agency systems;
“(4) identifying incidents quickly;
“(5) isolating and removing unauthorized entities from agency systems quickly;
“(6) otherwise increasing the resource costs for entities that cause incidents to be successful;
“(7) a summary of the agency progress reports required under subsection (b).

(b) AGENCY PROGRESS REPORTS.—Not later than 1 year after the date of enactment of this Act, the head of each agency shall submit to the Director a progress report on implementing an information security program based on the presumption of compromise and least privilege principles, which shall include—
“(1) a description of any steps the agency has completed, including progress toward achieving requirements issued by the Director;
“(2) an identification of activities that have not yet been completed and that would have the most immediate security impact; and
“(3) a schedule to implement any planned activities.

SEC. 5148. AUTOMATION REPORTS.

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

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

SEC. 5149. EXTENSION OF FEDERAL ACQUISITION SECURITY COUNCIL.

Section 1328 of title 41, United States Code, is amended by striking “the date that” and all that follows and inserting “December 31, 2026.”.

SEC. 5150. COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY DASHBOARD.

(a) DASHBOARD REQUIRED.—Section 11(e)(2) of the Inspector General Act of 1976 (1 U.S.C. App.) is amended—
“(1) in subparagraph (A), by striking “and” and inserting “or”;
“(2) by redesignating subparagraph (B) as subparagraph (C); and
“(3) by inserting after subparagraph (A) the following:
“(B) shall include a dashboard of open information and machine readable data that shall establish, review, and update metrics to track trends in the cybersecurity and infrastructure security response capabilities of the Cybersecurity and Infrastructure Security Agency that are available to the public in a way that is consistent with the requirements of section 3554 of title 44, United States Code; and
“(C) a description of any steps the agency has completed, including progress toward achieving requirements issued by the Director;”.

SEC. 5151. QUANTITATIVE CYBERSECURITY METRICS.

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

(b) UPDATING AND ESTABLISHING METRICS.—Not later than 1 year after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Director, shall—
“(1) evaluate any covered metrics established as of the date of enactment of this Act; and
“(2) as appropriate and pursuant to section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c))—
“(A) update the covered metrics; and
“(B) establish new covered metrics.

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

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

(e) PENETRATION TESTS.—On not less than 2 occasions during the 3 years that follow the date on which guidance is promulgated under paragraph (1), the Director shall ensure that not less than 3 agencies are subjected to substantially similar penetration tests, as determined by the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, in order to validate the utility of the covered metrics.

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

(g) CONGRESSIONAL REPORTS.—
“(1) UTILITY OF METRICS.—Not later than 1 year after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall submit to the appropriate congressional committees a report on the utility of the covered metrics.

(h) USE OF METRICS.—Not later than 180 days after the date of enactment of this Act, the Director shall submit to the appropriate congressional committees a report on the results of the use of the covered metrics by agencies.

(i) CYBERSECURITY ACT OF 2015 UPDATES.—Section 1204 of title 41, United States Code, (6 U.S.C. 1522) is amended—
“(1) by striking subsection (c) and inserting the following:
“(1) OMB REPORT.—Not later than 180 days after the date of enactment of this Act, the Comptroller General of the United States shall perform a study on the use of automation and machine readable data across the Federal Government for cybersecurity purposes, including the automated updating of cybersecurity tools, sensors, or processes by agency information systems.

(2) U.S. GOVERNMENT CIVILIAN INFORMATION SYSTEMS.—The term ‘appropriate congressional committees’ means—

TITLE LIII—RISK-BASED BUDGET MODEL

SEC. 5161. DEFINITIONS.

In this title—
“(a) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ‘appropriate congressional committees’ means—

SEC. 5162. RISK-ADJUSTED COSTS AND INNOVATION.
(A) the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate; and

(b) the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives.

(2) COVERED AGENCY.—The term ‘‘covered agency’’ has the meaning given the term ‘‘executive agency’’ in section 113 of title 41, United States Code.

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

(4) INFORMATION TECHNOLOGY.—The term ‘‘information technology’’—

(A) has the meaning given in the section in title 1101 of title 40, United States Code; and

(B) includes the hardware and software systems of a Federal agency that monitor and control physical equipment and processes of the Federal agency.

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

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

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

SEC. 5162. ESTABLISHMENT OF RISK-BASED BUDGET MODEL

(a) IN GENERAL.—

(1) MODEL.—Not later than 1 year after the first publication of the budget submitted by the President under section 1105 of title 31, United States Code, following the date of enactment of this Act, the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director and in coordination with the Director of the National Institute of Standards and Technology, shall develop a standard model for creating a risk-based budget for cybersecurity spending.

(2) RISK-BASED BUDGET MODEL.—Section 3553(a)(1) of title 44, United States Code, as amended by section 5121 of this Act, is further amended by inserting after paragraph (1)—

‘‘(2) a model to inform Federal agency cybersecurity budget development; and’’.

(3) PLAN.—The model required to be developed under paragraph (1) shall—

(A) consider Federal and non-Federal cyber threats, including the impact of cyber threat intelligence products, where available, to identify threats, vulnerabilities, and risks;

(B) consider the impact of agency operations on the interconnectivity of other agency systems and the operations of other agencies;

(C) indicate where resources should be allocated to protect against potential cyber threats; and

(D) include a plan for the sustainability of—

(i) information technology and cybersecurity tools;

(ii) information technology and cybersecurity architectures;

(iii) information technology and cybersecurity personnel; and

(iv) cybersecurity and information technology-related agreements and operations; and

(E) be evaluated to ensure appropriate coordination with the National Institute of Standards and Technology, in consultation with the Department of Commerce.

(4) REQUIRED USE OF RISK-BASED BUDGET MODEL.—

(1) IN GENERAL.—Not later than 2 years after the date on which the model developed under subsection (a) is published, the head of each covered agency shall use the model to develop the annual cybersecurity and information technology budget requests of the agency.

(2) AGENCY PERFORMANCE PLANS.—Section 3554(d)(2) of title 44, United States Code, is further amended by inserting ‘‘and the risk-based budget model required under section 3553(a)(2)’’ after ‘‘(paraphrase (1)’’.

(c) VERIFICATION.—

(1) RISK-BASED BUDGET.—Section 3555(a)(35)(A)(i)(V) of title 44, United States Code, is amended—

(A) by striking ‘‘by agency, and by initiative area (as determined by the administration)’’;

(B) by striking ‘‘and by initiative’’ after ‘‘agency’’;

(C) by striking ‘‘by agency, and by initiative area (as determined by the administration)’’;

(D) be used to inform acquisition and sustainment of—

(i) information technology and cybersecurity tools;

(ii) information technology and cybersecurity architectures;

(iii) information technology and cybersecurity personnel; and

(iv) cybersecurity and information technology-related agreements and operations; and

(E) be evaluated to ensure appropriate coordination with the National Institute of Standards and Technology, in consultation with the Department of Commerce.

(2) APPROPRIATE INTERAGENCY AGREEMENTS.—Not later than 1 year after the date on which the model developed under subsection (a) is published, the head of each covered agency shall submit to the appropriate congressional committees a report that includes—

(1) an evaluation of the success of covered agencies in developing risk-based budgets;

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

(3) an evaluation of whether the risk-based budgets developed by covered agencies mitigate cyber vulnerabilities, including the extent to which the risk-based budgets inform Federal Government-wide cybersecurity programs; and

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

TITLE LV.—PILOT PROGRAMS TO ENHANCE FEDERAL CYBERSECURITY

SEC. 5181. ACTIVE CYBER DEFENSIVE STUDY.

(a) DEFINITION.—In this section, the term ‘‘active defense technique’’ means—

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

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

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

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

(2) an evaluation of—

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

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

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

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

SEC. 5182. SECURITY OPERATIONS CENTER AS A SERVICE PILOT.

(a) PURPOSE.—The purpose of this section is for the Cybersecurity and Infrastructure Security Agency to run a security operations center on behalf of another agency, alleviating the need to duplicate this function at every agency, and empowering a greater centralized cybersecurity capability.

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

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

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

(2) staffing and resources; and

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

(d) PILOT PROGRAM.—

(1) IN GENERAL.—Not later than 180 days after the date on which the plan required—
under subsection (b) is developed, the Direc-
tor of the Cybersecurity and Infrastructure Secu-
rity Agency, in consultation with the Direc-
tor, shall enter into a 1-year agreement with
agencies to offer a security
ity operations center as a shared service.
(2) ADDITIONAL AGREEMENT.—After the
date on which the briefing required under
subsection (d) expires, the Director of the
Cybersecurity and Infrastructure Secu-
rity Agency shall provide to the Com-
mmittee on Homeland Security and Govern-
mental Affairs of the Senate and the Com-
mmittee on Homeland Security and the Com-
mmittee on Oversight and Reform of the House
of Representatives a briefing on the param-
eters of any 1-year agreements entered into
under subsection (d)(1).
(2) REPORT.—Not later than 90 days after
the date of enactment of this Act, the Direc-
tor of the Cybersecurity and Infrastructure Secu-
rity Agency shall submit to the Com-
mmittee on Homeland Security and Gov-
ernmental Affairs of the Senate and the Com-
mmittee on Homeland Security and the Com-
mmittee on Oversight and Reform of the House
of Representatives a report on—
(A) the agreement; and
(B) any additional agreements entered into
with agencies under subsection (d).
DIVISION F—CYBER INCIDENT REPORT-
ING ACT OF 2021 AND CISA TECHNICAL
CORRECTIONS AND IMPROVEMENTS
TITLE LXI—CYBER INCIDENT REPORTING
ACT OF 2021
SEC. 6101. SHORT TITLE.
This title may be cited as the “Cyber Inci-
dent Reporting Act of 2021”.
SEC. 6102. DEFINITIONS.
In this title:
(1) COVERED CYBER INCIDENT; COVERED ENTIT-
TY.—‘‘Covered cyber incident’’ and ‘‘covered
entity’’, and ‘‘cyber incident’’ have the mean-
gings given those terms in section 2230 of the Homeland
Security Act of 2002, as added by section 6103 of this title.
(2) DIRECTOR.—The term ‘‘Director’’ means
the Director of the Cybersecurity and Infra-
structure Security Agency.
(3) INFORMATION SYSTEM; RANSOM PAYMENT;
RANSOMWARE ATTACK; SECURITY VULNER-
ABILITY.—The terms ‘‘information system’’, ‘‘ransom
payment’’, ‘‘ransomware attack’’, and ‘‘security vulnerability’’
have the mean-
gings given those terms in section 2200 of the Homeland
Security Act of 2002, as added by section 6103 of this title.
SEC. 6103. CYBER INCIDENT REPORTING.
(a) CYBER INCIDENT REPORTING.—Title XXII
(1) in section 2209(b) (6 U.S.C. 659(b)), as so
redesignated by section 6203(b) of this divi-
sion—
(A) in paragraph (1), by striking the end and
inserting ‘‘; and’’; and
(C) by adding at the end the following:
‘‘(13) receiving, aggregating, and analyzing
reports related to covered cyber incidents (as
defined in section 2230) submitted by covered
entities relating to ransom payments and
reports related to ransom payments submitted
by entities in furtherance of the activities
specified in sections 220(e), 2203, and 2231,
this subsection, and any other authorized ac-
tivity of the Director, to enhance the situ-
atual awareness of cybersecurity threats across critical infrastructure sectors; and
(2) by adding at the end the following:
‘‘Subtitle C—Cyber Incident Reporting
SEC. 2230. DEFINITIONS.
‘‘In this subtitle:
(A) ‘‘Center’’ means the center established under section 2209.
(B) ‘‘Council’’—The term ‘‘Council’’ means the
Cyber Incident Reporting Council described in section 2209.
(C) ‘‘covered cyber incident’’ means a substantial
cyber incident experienced by a covered entity
that satisfies the definition and criteria established by the Director in the final
rule issued pursuant to subsection (b).
‘‘(4) ‘‘covered entity’’ means
(A) any Federal contractor; or
(B) an entity that owns or operates critical
infrastructure that satisfies the defini-
tion established by the Director in the final
rule issued pursuant to subsection (b).
‘‘(5) ‘‘cyber incident’’ has the meaning given the term ‘‘inci-
dent’’ in section 2230.
(1) REASONABLE.—The term ‘‘cyber threat’’—
(A) has the meaning given the term ‘‘cy-
bersecurity threat’’ in section 2200; and
(B) does not include any activity related to
good faith security research, including
participation in a bug-bounty program or a
vulnerability disclosure program.
‘‘(6) ‘‘Federal contractor’’—The term ‘‘Fed-
eral contractor’’ means a business, nonprofit
organization, or other private sector entity
that holds a Federal Government contract or
subcontract at any tier; grant, cooperative
agreement, or other transaction agreement,
unless that entity is a party only to—
(A) a service contract to provide house-
keeping or custodial services; or
(B) a contract to provide products or serv-
cices unrelated to information technology
that effectively covers a covered cyber
incident, as defined in section 2.101 of title 48, Code of Federal Regulations,
or any successor regu-
lation.
‘‘(7) ‘‘Federal entity; information system; secu-
rity control’’—The terms ‘‘Federal enti-
ty’’, ‘‘information system’’, and ‘‘security control’’ have the mean-
‘‘(8) ‘‘Significant cyber incident’’—The
term ‘‘significant cyber incident’’ means a cy-
ber incident by a group of related cyber
incidents that, Secretary determines
likely to result in demonstrable harm to the national security inter-
ests, foreign relations, or economy of the
United States or to the public confidence,
civil liberties, or public health and safety
of the people of the United States.
‘‘(9) ‘‘Small organization’’—The term
‘small organization’ means—
(A) means—
(i) a small business concern, as defined in
section 3 of the Small Business Act (15 U.S.C. 632); or
(ii) any nonprofit organization, including
faith-based organizations and houses of
worship, or any covered entity formed by
fewer than 200 employees (determined on a
full-time equivalent basis); and
(B) which includes—
(i) a business, nonprofit organization,
or other private sector entity that is a covered
entity; or
(‘‘ii) a Federal contractor.
‘‘SEC. 2231. CYBER INCIDENT REVIEW.
(‘‘a) ACTIVITIES.—The Center shall—
(1) receive, aggregate, analyze, and secure,
using processes consistent with the prin-
ciples developed pursuant to the Cyberse-
curity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.), reports from covered enti-
ties related to a cyber incident to as-
sume cyber threat indicators and other
cybersecurity purposes, including to
determine the effectiveness of controls,
to assess potential impact of incidents on
public health and safety, and to have a more
accurate picture of the cyber threat to criti-
cal infrastructure and the people of the
United States;
(2) receive, aggregate, analyze, and secure
reports to lead the identification of tactics,
techniques, and procedures used to perpet-
uate cyber incidents and ransomware at-
tacks;
(3) coordinate and share information with
appropriate Federal departments and a-
genies to identity and track ransom payments, including those utilizing virtual currencies;
(4) leverage information gathered about
cyber vulnerabilities in industry,
including agencies, sector coordinating councils,
information sharing and analysis organizations, technology providers, critical infrastructure owners and operators, cybersecurity and inci-
dent response firms, and security research-
ers; and
(5) provide appropriate entities, includ-
ing agencies, sector coordinating councils,
information sharing and analysis organiza-
tions, technology providers, cybersecurity and incident response firms, and security re-
searchers, with timely, actionable, and
anonymized reports of cyber incident cam-
paigns and trends, including, to the max-
imum extent practicable, related contextual
information, cyber threat indicators, and de-
fensive measures, pursuant to section 2235;
(5) establish mechanisms to receive feed-
back from stakeholders on how the Agency
communicates, sector coordinating councils,
information sharing and analysis organiza-
tions, technology providers, cybersecurity and incident response firms, and security re-
searchers, with timely, actionable, and
anonymized reports of cyber incident cam-
paigns and trends, particularly with respect
to reducing cyber security vulnerabilities and identify and disseminate ways to prevent or mitigate similar incidents in the future;
(6) (A) for a covered cyber incident, including
a ransomware attack, that also satisfies the
definition of a significant cyber incident, or
is part of a group of related cyber incidents
that the other satisfy that condi-
tion, conduct a review of the details surrounding the
covered cyber incident or group of those inci-
dents and identify and disseminate ways to prevent or mitigate similar incidents in the future;
(6) (B) with respect to covered cyber incident
reports under section 2232(a) and 2233 invol-
involving an ongoing cyber threat or security vul-
nery, immediately review those reports
for cyber threat indicators that can be
anonymized and disseminated, with defen-
sive measures, to appropriate stakeholders,
in coordination with other divisions within
the Agency, as appropriate;
(9) publish quarterly unclassified, public reports
that may include declassified information contained in the briefings
required under subsection (c);
"(10) proactively identify opportunities and perform analyses, consistent with the protections in section 2235, to leverage and utilize data on ransomware attacks to support law enforcement operations to identify, track, and seize ransom payments utilizing virtual currencies, to the greatest extent practicable;"

"(11) in accordance with section 2235 and subsection (b) of this section, as soon as possible but not later than 24 hours after receiving a covered cyber incident report, ransom payment reports, or a required ransom payment report required under paragraph (1), the Cyber Director shall make available to appropriate Sector Risk Management Agencies and other appropriate Federal agencies;"

"(b) INTERAGENCY SHARING.—The National Cyber Director, in consultation with the Director and the Director of the Office of Management and Budget—"

"(1) may establish a specific time requirement for sharing information under subsection (a)(13); and"

"(2) shall determine the appropriate Federal agencies under subsection (a)(13)."

"(c) NOTIFICATION.—Not later than 10 days after the effective date of the final rule required under section 2232(b), and on the first day of each month thereafter, the Director, in consultation with the National Cyber Director, the Attorney General, and the Director of National Intelligence, shall provide to the majority leader of the Senate, the Speaker of the House of Representatives, the minority leader of the House of Representatives, the Chairman on Homeland Security and Governmental Affairs of the Senate, and the Chairman of Homeland Security of the House of Representatives a briefing that characterizes the national cyber threat landscape, threat faced by Federal agencies and covered entities, and applicable intelligence and law enforcement information, covered cyber incidents, and ransomware attacks, as of the date of the briefing, which shall—"

"(1) include the total number of reports submitted under sections 2232 and 2233 during the month, including breakdowns of required and voluntary reports;"

"(2) include any identified trends in covered cyber incidents and ransomware attacks over the course of the preceding month and as compared to previous reports, including any trends related to the information collected in the reports submitted under sections 2232 and 2233, including the Senate, the Speaker, the House of Representatives, the National Cyber Director, the Attorney General, and the Director of National Intelligence;"

"(3) include a summary of the known uses of the information in reports submitted under sections 2232 and 2233; and"

"(4) be unclassified, but may include a classified annex.

"SEC. 2232. REQUIRED REPORTING OF CERTAIN CYBER INCIDENTS.

"(a) IN GENERAL.—"

"(1) COVERED CYBER INCIDENT REPORTS.—A covered entity that is a victim of a covered cyber incident shall report the covered cyber incident to the Director not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred."

"(2) RANSOM PAYMENT REPORTS.—An entity, including a covered entity and except for an individual or a small organization, that makes a ransom payment or the result of a ransomware attack against the entity shall report the payment to the Director not later than 24 hours after the ransom payment has been made.

"(3) SUPPLEMENTAL REPORTS.—A covered entity shall promptly submit to the Director an update or supplement to a previously submitted covered cyber incident report if new or different information becomes available or if the covered entity makes a ransom payment after submitting a covered cyber incident report required under paragraph (1).

"(4) PRESERVATION OF INFORMATION.—Any entity subject to requirements of paragraphs (1), (2), and (3) shall retain all information relevant to the covered cyber incident or ransom payment in accordance with procedures established in the final rule issued pursuant to subsection (b)."

"(5) EXCEPTIONS.—"

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

"(B) SUBSTANTIALLY SIMILAR REPORTED INFORMATION.—The requirements under paragraphs (1), (2), and (3) shall not apply to an entity required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe.

"(C) DOMAIN NAME SYSTEM.—The requirements under paragraphs (1), (2), and (3) shall not apply to an entity that is a domain name system (DNS) provider, or other third-party data hosting provider, or a domain name system registry, for purposes of reporting DNS activity to the Director.

"(D) MANNER, TIMING, AND FORM OF REPORTS.—Reports made under paragraphs (1), (2), and (3) shall be made in the manner and form, and within the time period in the case of reports made under paragraph (3), prescribed in the final rule issued pursuant to subsection (b).

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

"(F) RULEMAKING.—Not later than 2 years after the date of enactment of this section, the Director, in consultation with Sector Risk Management Agencies, the Department of Justice, and other Federal agencies, shall publish in the Federal Register a notice of proposed rulemaking to implement subsection (a).

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

"(H) SUBSEQUENT RULEMAKINGS.—

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

"(2) PROCEDURES.—Any subsequent rules issued under subparagraph (A) shall comply with the requirements under chapter 5 of title 5, including the issuance of a notice of proposed rulemaking under section 553 of such title.

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

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

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

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

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

"(ii) a disruption of business or industrial operations due to a cyber incident; or"

"(iii) an occurrence described in clause (I) or (II) due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise;"

"(J) consider—"

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

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

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

"(K) include—"

"(i) any event where the cyber incident is perpetuated by good faith security research or in response to an invitation by the owner or operator of the information system for the purpose of testing the effectiveness of the information system, such as through a vulnerability disclosure program or the use of authorized penetration testing services; and"

"(ii) the threat of disruption as extortion, as described in section 2201(9)(A).

"(L) A clear description of the specific required contents of a report pursuant to section (a)(1), which shall include the following:

"(I) the information that is attributable and available, with respect to a covered cyber incident:
“(A) A description of the covered cyber incident, including—
   "(i) identification and a description of the function of the affected information systems, networks, or services that were, or are reasonably believed to have been, affected by such incident;
   "(ii) a description of the unauthorized access or substantial loss of confidentiality, integrity, or availability of the affected information system or network or disruption of business or industrial operations;
   "(iii) an estimated date range of such incident; and
   "(iv) the impact to the operations of the covered entity;
   "(B) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetuate the covered cyber incident;
   "(C) Where applicable, any identifying or contact information related to each actor reasonably believed to be responsible for such incident.
   "(D) Where applicable, identification of the category or categories of information that were, or are reasonably believed to have been, accessed or acquired by an unauthorized person.
   "(E) The name and other information that clearly identifies the entity impacted by the covered cyber incident;
   "(F) Contact information, such as telephone number or electronic mail address, that the Center may use to contact the covered entity or an authorized agent of such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission of, and at the direction of, the covered entity to assist with compliance with the requirements of this subtitle.
   "(G) A clear description of the specific required contents of a report pursuant to subsection (a)(2), which shall be the following information, to the extent applicable and available, with respect to a ransom payment:
      "(1) A description of the ransomware attack, including the estimated date range of the attack.
      "(2) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetuate the ransomware attack.
      "(3) Where applicable, any identifying or contact information related to the actor or actors reasonably believed to be responsible for the ransomware attack.
      "(4) The name and other information that clearly identifies the entity that made the ransom payment.
      "(5) Voluntary information, such as telephone number or electronic mail address, that the Center may use to contact the entity that made the ransom payment or an authorized agent of such entity, or, where applicable, the service provider of such covered entity acting with the express permission of, and at the direction of, such entity, to assist with compliance with the requirements of this subtitle.
      "(6) The date of the ransom payment.
      "(7) The ransom payment demand, including the amount of virtual currency or other commodity requested, if applicable.
      "(H) The ransom payment instructions, including the manner and form thereof, which shall include, at a minimum, a concise, user-friendly web-based form;
      "(I) The Agency to carry out the enforce-ment provisions of section 2233, including with respect to the issuance, service, withdrawal, and enforcement of subpoenas, appeals and due process procedures, the suspension and debarment provisions in section 2234, and other matters of noncompliance;
      "(J) Implementing the exceptions provided in subsection (a) of section 2232.
      "(K) Procedures for—
         "(a) entities to submit reports required by paragraph (g) of subsection (a), including the manner and form thereof, which shall include, at a minimum, a concise, user-friendly web-based form;
         "(b) the Agency to carry out the enforcement provisions of section 2233, including with respect to the issuance, service, withdrawal, and enforcement of subpoenas, appeals and due process procedures, the suspension and debarment provisions in section 2234, and other matters of noncompliance;
   "(C) implementing the exceptions provided in subsection (a) of section 2232.
   "(D) protecting privacy and civil liberties consistent with processes adopted pursuant to section 16(b) of the Cybersecurity Act of 2015 (6 U.S.C. 1504(b)), anonymizing and safeguarding, or no longer retaining, information received and disclosed through covered cyber incident reports and ransom payment reports that is known to be personal information of a specific individual or information that identifies a specific individual that is not directly related to a cybersecurity threat;
   "(E) an overview of the final rule issued under section 2232(a) fails to comply with the require-ments under paragraphs (1), (2), and (3) of section 2232(a), and may enhance the situational awareness of cyber threats.
"SEC. 2234. NONCOMPLIANCE WITH REQUIRED REPORTING.
   "(a) PURPOSE.—In the event that an entity that is required to submit a report under sec- tion 2232(a) fails to comply with the require-ments to report, the Director may obtain infor-mation about the incident or ransom payment by engaging the entity directly if the entity requests information about the incident or ransom payment, and if the Director is unable to obtain information through such engage-ments, issue a subpoena to the entity, pursuant to section (c), to gather information sufficient to determine whether a
covered cyber incident or ransom payment has occurred, and, if so, whether additional action is warranted pursuant to subsection (d).

(2) INITIAL REQUEST FOR INFORMATION.—

(1) IN GENERAL.—If the Director has reason to believe, whether through public reporting or investigation in the performance of the functions of the Federal Government, including through analysis performed pursuant to paragraph (1) or (2) of section 2232(a), that an entity has experienced a covered cyber incident or made a ransom payment but failed to report such incident or payment to the Center within 72 hours in accordance with section 2232(c), the Director shall request additional information from the entity to confirm whether or not a covered cyber incident or ransom payment has occurred.

(2) Information provided to the Center in response to a request under paragraph (1) shall be treated as if it was submitted through the reporting procedures established in section 2232.

(3) AUTHORITY TO ISSUE SUBPOENAS AND DEBAR.—

(1) IN GENERAL.—If, after the date that is 72 hours from the date on which the Director made the request for information in subsection (b), the Director has received no response from the entity from which such information was requested, or received an inadequate response, the Director may issue to such entity a subpoena to compel disclosure of information the Director determines necessary to determine whether a covered cyber incident or ransom payment has occurred and obtain the information required to be reported pursuant to section 2232 and any implementing regulations.

(2) CIVIL ACTION.—

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

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

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

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

(4) DEBARMENT OF FEDERAL CONTRACTORS.—If an entity has experienced a covered cyber incident that is a Federal contractor fails to comply with a subpoena issued under this subsection—

(A) the Director may refer the matter to the Administrator of General Services; and

(B) upon receiving a referral from the Director, the Administrator of General Services may impose additional available penalties, including suspension or debarment.

(5) AUTHENTICATION.—

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

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

(d) ACTIONS BY ATTORNEY GENERAL AND FEDERAL REGULATORY AGENCIES.—

(1) AUTHORIZATION FOR SUBPOENAS.—A covered cyber incident or ransom payment report submitted to the Center by an entity that makes a ransom payment or third party under section 2232 shall be retained by the Federal Government in accordance with this subtitle.

(2) AUTHENTICATION.—

(A) IN GENERAL.—Any subpoena issued pursuant to subsection (c), that fact relating to the covered cyber incident or ransom payment at issue may constitute grounds for a regulatory enforcement action or criminal prosecution, the Attorney General or the appropriate Federal regulatory agency may take action for a regulatory enforcement action or criminal prosecution.

(B) APPLICATION TO CERTAIN ENTITIES AND THIRD PARTIES.—A covered cyber incident or ransom payment report submitted to the Center by an entity that makes a ransom payment or third party under section 2232 shall be retained by the Federal Government in accordance with this subtitle.

(C) RULE OF CONSTRUCTION.—Nothing in this subtitle shall be construed to provide an entity that submits a covered cyber incident report or ransom payment report under section 2232 any immunity from law enforcement action for making a ransom payment otherwise prohibited by law.

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

(1) the size and complexity of the entity;

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

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

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

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

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

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

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

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

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

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

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

SEC. 2235. INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.

(a) DISCLOSURE, RETENTION, AND USE.—

(1) AUTHORIZED ACTIVITIES.—Information provided to the Center or Agency pursuant to section 2232 or 2233 may be disclosed by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

(A) a cybersecurity purpose;

(B) the purpose of identifying—

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

(ii) a security vulnerability; and

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

(D) the purpose of responding to, investigating, prosecuting, or otherwise preventive measures related to mitigating, a ransom payment to a minor, including sexual exploitation and threats to physical safety; or

(E) the purpose of preventing, investigating, or otherwise mitigating, an offense arising out of a cyber incident reported pursuant to section 2232 or 2233 or any of the offenses listed in section 105(d)(5)(A)(v) of the Cybersecurity Act of 2015 (6 U.S.C. 1504(h)(5)(A)(v)).

(2) AGENCY ACTIONS AFTER RECEIPT OF SUBPOENA.—

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

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

(c) EXEMPTION FROM DISCLOSURE.—Information contained in covered cyber incident and ransom payment reports submitted to the Center or the Agency pursuant to section 2232 shall be retained, used, and disseminated, where permissible and appropriate, by the Federal Government in accordance with processes to be developed for the protection of personal information consistent with processes adopted pursuant to section 105 of the Cybersecurity Act of 2015 (6 U.S.C. 1504) and in a manner that protects from unauthorized use or disclosure any information that may contain—

(A) personal information of a specific individual;

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

(d) PROHIBITION ON USE OF INFORMATION IN REGULATORY ACTIONS.—A Federal, State, or Tribal government may use information about a covered cyber incident or ransom payment obtained solely through reporting directly to the Center or the Agency in accordance with this subtitle, including through an enforcement action, the activities of the covered entity or entity that made a ransom payment.

(e) NO WAIVER OF PRIVILEGE OR PROTECTION.—The submission of a report to the Center or the Agency under section 2232 shall not constitute a waiver of any applicable privileges or protections under law, including trade secret protection and attorney-client privilege.

(f) EXEMPTION FROM DISCLOSURE.—Information contained in a report submitted to the Office under section 2232 shall be exempt from disclosure.
from disclosure under section 552(b)(3) of title 5, United States Code (commonly known as the ‘Freedom of Information Act’) and any State, Tribal, or local provision of law requiring disclosure of information or records.

“(d) Ex Parte Communications.—The submission of a report to the Agency under section 2232(a)(1) that relating to a report from an entity of a cyber incident, including a ransomware attack, shall provide the report to the Director as soon as possible but not later than 24 hours after receiving the report, unless a shorter period is required by an agreement made between the Cybersecurity Infrastructure Security Agency and any other party. The Director shall share and coordinate each report pursuant to section 2231(b) of the Homeland Security Act of 2002, as added by section 6193 of this title.

(2) RULE OF CONSTRUCTION.—The requirements described in paragraph (1) shall not be construed to be a violation of any provision of law or policy that would otherwise prohibit disclosure within the executive branch.

(3) PROTECTION OF INFORMATION.—The Director shall comply with any obligations of the Department or agency described in paragraph (1) to protect information, including with respect to privacy, confidentiality, or information security, if those obligations would otherwise be construed to be a violation of any provision of law or policy that would otherwise prohibit disclosure within the executive branch.

(4) FOIA EXEMPTION.—Any report received by the Director pursuant to paragraph (1) shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code (commonly known as the ‘Freedom of Information Act’).

(b) CREATION OF COUNCIL.—Section 1752(c) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500) is amended—

(1) in paragraph (1)—

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

(2) N O IDENTIFICATION.—If the Director is not able to identify the entity at risk that owns or operates a vulnerable information system identified in subsection (b), the Director shall comply with any obligations of the Department or agency described in paragraph (1) to protect information, including with respect to privacy, confidentiality, or information security, if those obligations would otherwise be construed to be a violation of any provision of law or policy that would otherwise prohibit disclosure within the executive branch.

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

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

(2) RULE OF CONSTRUCTION.—Nothing in paragraph (1) shall be construed to be a violation of any provision of law or policy that would otherwise prohibit disclosure within the executive branch.

(3) RULE OF CONSTRUCTION.—Nothing in paragraph (1) shall be construed to be a violation of any provision of law or policy that would otherwise prohibit disclosure within the executive branch.

(g) TERMINATION.—The pilot program established under subsection (a) shall terminate on the date that is 4 years after the date of enactment of this Act.
Task Force to coordinate an ongoing nationwide campaign against ransomware attacks, and identify and pursue opportunities for international cooperation.

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

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

(A) Prioritization of Intelligence-driven Operations to disrupt specific ransomware actors.

(B) Consult with relevant private sector, State, local, Tribal, and territorial governments and international stakeholders to identify needs and establish mechanisms for providing input into the Task Force.

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

(i) prioritization for Federal action by appropriate agencies and sectors.

(ii) Identify metrics for success of said actions.

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

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

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

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

(H) Any other activities determined appropriate by the task force to mitigate the threat of ransomware attacks against Federal and non-Federal entities.

(b) CLARIFYING PRIVATE SECTOR LAWFUL DEFENSIVE MEASURES.—Not later than 180 days after the date of enactment of this Act, the National Cyber Director, in coordination with the Secretary of Homeland Security and the Attorney General, shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Homeland Security and Governmental Affairs of the Senate the following report describing how the National Cybersecurity and Communications Integration Center established under section 6106 of the Homeland Security Act of 2002 (6 U.S.C. 659) has carried out activities under section 2231(a)(9) of the Homeland Security Act of 2002, as added by section 6103(a) of this title:

(1) A list of duplicative Federal cyber incident reporting requirements on covered entities and entities that make a ransom payment;

(2) A description of any challenges in harmonizing the duplicative reporting requirements;

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

(4) To the extent practicable, the number of vulnerable systems mitigated under this pilot by the Agency during the preceding year.

(d) REPORT ON HARMONIZATION OF REPORTING REGULATIONS.—

(1) IN GENERAL.—Not later than 180 days after the date on which the National Cyber Director convenes the Council described in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)), the National Cyber Director shall submit to the appropriate congressional committees a report that includes—

(A) a list of duplicative Federal cyber incident reporting requirements on covered entities and entities that make a ransom payment;

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

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

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

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

(g) GAO REPORTS.—

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

(2) EXEMPTIONS TO REPORTING.—Not later than 1 year after the date on which the Director issues the final rule under section 2232(b) of the Homeland Security Act of 2002, as added by section 6103 of this title, which shall include—

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

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

(C) an evaluation of the burden, financial and otherwise, on entities required to report cyber incidents under this Act, including an analysis of entities that meet the definition of a small organization and would be exempt from ransom payment reporting but not for being a covered entity; and

(D) a description of the consequences and effects of the exemptions.

(f) REPORT ON EFFECTIVENESS OF ENFORCEMENT MECHANISMS.—Not later than 1 year after the date on which the Director issues the final rule required under section 2232(b) of the Homeland Security Act of 2002, as added by section 6103 of this title, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the effectiveness of the enforce- ment mechanisms within section 2231 of the Homeland Security Act of 2002, as added by section 6103 of this title.

TITLE LXII—CISA TECHNICAL CORRECTIONS AND IMPROVEMENTS ACT OF 2021

SEC. 6201. SHORT TITLE.

This title may be cited as the "CISA Technical Corrections and Improvements Act of 2021".

SEC. 6202. REDESIGNATIONS.

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

(1) by redesignating section 2217 (6 U.S.C. 665f) as section 2220;

(2) by redesigning section 2216 (6 U.S.C. 665e) as section 2219;

(3) by redesigning the fourth section 2215 (relating to Sector Risk Management Agencies) (6 U.S.C. 665d) as section 2217;

(4) by redesigning the third section 2215 (relating to the Cybersecurity State Coordinator) (6 U.S.C. 665c) as section 2216;

(b) TECHNICAL AND CONFORMING AMENDMENTS.—Section 2202(c) of the Homeland Security Act of 2002 (6 U.S.C. 652(c)) is amended—

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

(2) in the first paragraph (12)—

(A) by striking "section 2215" and inserting "section 2217"; and

(B) by striking "and" at the end; and

(3) by redesigning the second and third paragraphs (12) as paragraphs (13) and (14), respectively.

(c) ADDITIONAL TECHNICAL AMENDMENT.—


(2) EFFECTIVE DATE.—The amendment made by paragraph (1) shall take effect as if enacted as part of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260).
SEC. 6203. CONSOLIDATION OF DEFINITIONS.

(a) IN GENERAL.—Title XXII of the Home-
land Security Act of 2002 (6 U.S.C. 651) is amended by inserting before the subtitl-
e A heading:

“SEC. 2200. DEFINITIONS.

Except as otherwise specifically provided, in this title:

(1) AGENCY.—The term ‘Agency’ means the
Homeland Security and Infrastructure Secu-
ritv Agency.

(2) AGENCY INFORMATION.—The term
agency information’ means information col-
clected or maintained by or on behalf of an
agency.

(3) AGENCY INFORMATION SYSTEM.—The
term ‘agency information system’ means an
information system used or operated by an
agency or by another entity on behalf of an
agency.

(4) APPROPRIATE CONGRESSIONAL COMMIT-
tees.—The term ‘appropriate congressional
committees’ 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.

(5) CLOUD SERVICE PROVIDER.—The term
‘cloud service provider’ means an entity off-
ering cloud computing services related to cloud
computing, as defined by the National Insti-
tutes of Standards and Technology in NIST
Special Publication 800-145 and any amend-
tory or superseding document relating thereto.

(6) CRITICAL INFRASTRUCTURE INFOR-
MATION.—The term ‘critical infrastructure
information’ means information not custom-
arily in the public domain and related to the
security of critical infrastructure or pro-
tected systems, including—

(A) actual, potential, or threatened inter-
ference with, attack on, compromise of, or
incapacitation of critical infrastructure or
protected systems by either physical or com-
puter-based attack or other similar conduct
(including the misuse of or unauthorized ac-
cess to all types of communications and data
transmission systems) that violates Federal,
State, or local law, harms interstate com-
merce of the United States, or threatens public
health or safety;

(B) The ability of any critical infrastruc-
ture or protected system to resist such inter-
ference, compromise, or incapacitation, in-
cluding any planned or past assessment, pro-
jection of the vulnerability of critical infra-
structure or a protected system, including
security testing, risk evaluation thereto, risk
management planning, or risk audits;

(C) any planned or past operational prob-
lem or solution regarding critical infrastruc-
ture or protected systems, including repair,
reconstruction, insurance, or continu-
tuity, to the extent it is related to such inter-
ference, compromise, or incapacitation.

(7) CYBER THREAT INDICATOR.—The term
‘cyber threat indicator’ means information
that is necessary to describe or identify—

(A) malicious reconnaissance, including
anomalous patterns of communications that
appear to be transmitted for the purpose of
gathering technical information related to a
cybersecurity threat or security vulner-
ability;

(B) a method of defeating a security con-
tral or exploitation of a security vulner-
ability;

('E) malicious cyber command and con-
tr;

(F) the actual or potential harm caused
by an incident, including a description of the
information exfiltrated as a result of a par-
ticular cybersecurity threat;

(G) any instance of a cybersecurity threat,
if disclosure of such attribute is not
otherwise prohibited by law; or

(H) any combination thereof.

(8) CYBERSECURITY.—The term
‘cybersecurity’ purpose’ means the purpose
of protecting an information system or infor-
mation that is stored on, processed by, or
transiting an information system from a cy-
bersecurity threat.

(9) CYBERSECURITY RISK.—The term ‘cy-
bersecurity risk’ means—

(A) means threats to and vulnerabilities
of information or information systems and
any related consequences caused by or re-
sulting from unauthorized access, use, dis-
closure, degradation, disruption, modifica-
tion, or destruction of such information or
information systems, including such related
consequences caused by an act of terrorism;
and

(B) does not include any action that solely
involves a violation of a consumer term of
service or a contract agreement.

(10) CYBERSECURITY THREAT.—

(A) IN GENERAL.—Except as provided in
paragraph (B), the term ‘cybersecurity threat’
means any measure that is protected by the
First Amendment of the Constitution of the
United States, or on or through an informa-
tion system that may result in an unauthor-
ized effort to adversely impact the security,
availability, confidentiality, or integrity of an
information system or information that is
stored on, processed by, or transiting an infor-
mation system.

(B) EXCLUSION.—The term ‘cybersecurity
threat’ does not include any action that solely
involves a violation of a consumer term of
service or a consumer licensing agreement.

(11) DEFENSIVE MEASURE.—

(A) IN GENERAL.—Except as provided in
paragraph (B), the term ‘defensive measure’
means an action, device, procedure, sig-
nature, technique, or other measure applied
to an information system or information
activity that is a state or non-state actor’s
tactic of cyberattacks, including—

(i) an information system or information
activity that detects, prevents, or mitigates
a known or suspected cyber-
security threat or cybersecurity
defense vulnerability;

(ii) an information system or information
activity that detects, prevents, or mitigates
a known or suspected cyber-
security threat or cybersecurity
defense vulnerability.

(B) EXCLUSION.—The term ‘defensive
measure’ does not include a measure that de-
stroys, renders unusable, provides unautho-
rized access to, or otherwise adversely affects
an information system or information that is
stored on, processed by, or transiting such
information system not owned by—

(i) the entity operating the measure; or

(ii) another entity or Federal entity that is
authorized to provide consent and has pro-
vided consent to that private entity for oper-
ation such measure.

(12) HOMELAND SECURITY ENTERPRISE.—
The term ‘Homeland Security Enterprise’
means relevant governmental and non-
governmental entities involved in homeland
security, including Federal, State, local, and
Tribal government officials, private sector re-
presentatives, academics, and other policy
experts.

(13) INCIDENT.—The term ‘incident’ means
an occurrence that actually or imminently
involves a violation of a consumer term of
service or a contract agreement.

(14) INTELLIGENCE COMMUNITY.—The
term ‘intelligence community’ has the meaning
given the term in section 3(4) of the National
Security Act of 1947 (50 U.S.C. 3003(4)).

(15) INTELLIGENCE COMMUNITY ORGAN-:
The term ‘intelligence community organ-
ization’ means a formal or informal entity
created or employed by public or private sec-
tor organizations, for purposes of—

(A) gathering and analyzing critical infra-
structure information related to cybersecurity risks and inci-
dents, in order to better understand security
problems and interdependencies related to
cybersecurity risks and incidents, to protect critical infra-
structure risks and incidents, and protected sys-
tems, so as to ensure the availability, integ-
ry, and reliability thereof;

(B) Voluntarily disseminating critical infra-
structure information, including cybersecurity
risks and incidents, to its members,
State, local, and Federal Governments, or
any other entities that may be of assistance
in carrying out the purposes specified in sub-
paragraphs (A) and (B).

(16) INFORMATION SYSTEM.—The term
‘information system’ has the meaning given
the term in section 3502 of title 44, United States
Code.

(17) MONITOR.—The term ‘monitor’ means
acquire, identify, or scan, or to possess,
information that is stored on, processed by,
or transiting an information system.

(18) NATIONAL CYBERSECURITY ASSET
RESPONSE ACTIVITIES.—The term ‘national cy-
bersecurity asset response activities’ means—

(A) furnishing cybersecurity technical as-

tance to entities affected by cybersecurity risks for the purpose of mitigating vulnerabilities, and reduce impacts of cyber incidents;

(B) identifying other entities that may be at risk of an incident and assessing risk to the same or similar vulnerabilities;

(C) assessing potential cybersecurity risks to a sector or region causing potential cascading effects, and developing courses of action to mitigate such risks;

(D) facilitating information sharing and operational coordination with threat response; and

(E) providing guidance on how best to uti-

lize Federal resources and capabilities in a timely, effective manner to speed recovery from cybersecurity risks.

(19) NATIONAL SECURITY SYSTEM.—The
term ‘national security system’ has the
meaning given the term in section 11103 of
title 40, United States Code.

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

(21) RANSOMWARE.—The term
‘ransomware’ attack—

(A) means a cyber incident that includes
the threat of ransomware or malicious code on an information system, or the use or threat of use of another digital

mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of data maintained on, processed by, or transmitted an information system to extort a demand for a ransom payment; and

(2) does not include any such event where the damage is caused by a Federal Government entity, good faith security research, or in response to an invitation by the owner or operator of the information system for third parties to identify vulnerabilities in the information system.

(22) SECTOR RISK MANAGEMENT AGENCY.—The term ‘Sector Risk Management Agency’ means the Office of Cybersecurity and Communications, designated by law or Presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all-hazards environment in coordination with the Department.

(24) SECURITY CONTROL.—The term ‘security control’ means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

(25) SECURITY VULNERABILITY.—The term ‘security vulnerability’ means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

(26) SHARING.—The term ‘sharing’ (including all conjugations thereof) means providing, receiving, and disseminating (including all conjugations of each such term).

(27) SUPPLY CHAIN COMPROMISE.—The term ‘supply chain compromise’ means a cyber incident within the supply chain of an information technology advisory can leverage to jeopardize the confidentiality, integrity, or availability of the information technology system or the information the system processes, stores, or transmits, and can occur at any point during the life cycle.

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

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

(b) TECHNICAL AND CONFORMING AMENDMENTS.—The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

(1) by amending section 2201 to read as follows:

‘‘SEC. 2201. DEFINITION.’’—In this subtitle, the term ‘Cybersecurity Advisory Committee’ means the advisory committee established under section 2219(a).

(2) in section 2202—

(A) in subsection (a)(1), by striking ‘‘this subtitle referred to as the ‘Agency’’; (B) by redesigning subsections (b) through (o) as subsections (a) through (n), respectively;

(C) in subsection (c)(1)—

(i) in subparagraph (A), as so redesignated, by striking ‘‘Assistant Director’’; and

(ii) in paragraphs (2) through (o), by redesigning ‘‘the Assistant Director’’; (B) in subsection (d), as so redesignated—

(i) in the matter preceding paragraph (1), by striking ‘‘subsection (c)’’ and inserting ‘‘subsection (b)’’; and

(ii) in subparagraph (B), by striking ‘‘the Assistant Director’’ and inserting ‘‘the Executive Director’’; (C) by redesigning paragraphs (2) through (o) as paragraphs (2) through (o), respectively.

(c) TABLE OF CONTENTS AMENDMENTS.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended—

(1) by inserting before the item relating to subtitle A of title XXI the following:

‘‘Sec. 2200. Definitions.’’; and

(2) by striking the item relating to section 2201 and inserting the following:

‘‘Sec. 2201. Definitions.’’; and

(3) by striking the item relating to section 2204 and all that follows through the item relating to section 2217 and inserting the following:


(d) CYBERSECURITY ACT OF 2015 DEFINITIONS.—Section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501) is amended—

(1) by striking paragraphs (4) through (7) and inserting the following:

‘‘(4) CYBERSECURITY PURPOSE.—The term ‘cybersecurity purpose’ has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

(5) CYBERSECURITY THREAT.—The term ‘cybersecurity threat’ has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

(6) CYBER THREAT INDICATOR.—The term ‘cyber threat indicator’ has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

(7) DEFENSIVE MEASURE.—The term ‘defensive measure’ has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

(8) CYBER SECURITY CONTROL.—The term ‘security control’ has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

(9) SECURITY VULNERABILITY.—The term ‘security vulnerability’ has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

(e) FEDERAL CYBERSECURITY ENHANCEMENT ACT OF 2015.—The Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1291 et seq.) is amended—

(1) in section 222 (6 U.S.C. 1291)—

(A) in paragraph (2), by striking ‘‘section 2210’’ and inserting ‘‘section 2200’’; and

(B) in paragraph (4), by striking ‘‘section 2209’’ and inserting ‘‘section 2208’’.

(2) in section 2223 (6 U.S.C. 1291 note), by striking ‘‘section 2213(b)(1)’’ each place it appears and inserting ‘‘section 2213(a)(1)’’;
(3) in section 226 (6 U.S.C. 1524)—
(A) in subsection (a)—
(1) in paragraph (1), by striking “section 2213” and inserting “section 2220”;
(2) in subsection (b)(2), by striking “section 2202” and inserting “section 2200 of the Homeland Security Act of 2002”;
(3) in subsection (c), by striking “section 2201(5)” and inserting “section 2200”;
(4) in subsection (d)(1), by striking “section 2218” and inserting “section 2215”;
(5) by striking “, as added by this section”;
(d) NATIONAL SECURITY ACT OF 1947.—Section 113B of the National Security Act of 1947 (50 U.S.C. 403b-1) is amended by striking “section 2202 of the Homeland Security Act of 2002.”;
(e) INTERNATIONAL SECURITY RISK MANAGEMENT ACT OF 2005.—Section 503(10) of the International Security Risk Management Act of 2005 (10 U.S.C. 1233) is amended by striking “the Director an application for an exemption” and inserting “the head of the agency personally certifies to the Director an application for an exemption”;
(f) IN GENERAL.—Not later than 30 days after the date of the enactment of this Act, the Secretary of the Treasury, subject to subsection (c) and (d) and any other provision of law, shall make available, from unobligated balances remaining available from fees collected before October 1, 2020, and credited to the Travel Promotion Fund established under subsection (d) of the Travel Promotion Act of 2009 (22 U.S.C. 213(d)), $250,000,000 for the Corporation for Travel Promotion (commonly known as “Brand USA”).
(g) INAPPLICABILITY OF CERTAIN REQUIREMENTS AND LIMITATIONS.—The limitations in subsection (d)(2)(B) of the Travel Promotion Act of 2009 shall not apply to amounts made available under subsection (b), and the requirements in subsection (d)(3) of such Act shall not apply to more than $50,000,000 of the amounts so available.

SEC. 1004. AVAILABILITY OF TRAVEL PROMOTION FUND FOR BRAND USA.

(a) SHORT TITLE.—This section may be called the “Restoring Freedom to Travel Act.”
(b) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the President shall submit to Congress a plan for obligating and expending the amounts described in subsection (b).

SA 4801. Mr. KENNEDY submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 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:

SEC. 3. SBIR and STTR PILOT PROGRAM FOR UNDERPERFORMING STATES.

Section 9 of the Small Business Act (15 U.S.C. 638) is amended by adding at the end the following:

“(vii) DEPARTMENT OF DEFENSE PILOT PROGRAM FOR UNDERPERFORMING STATES.—
(1) DEFINITIONS.—In this section:
(A) DEPARTMENT.—The term ‘Department’ means the Department of Defense.
(B) UNDERPERFORMING STATE.—The term ‘underperforming State’ means any State participating in the SBIR or STTR programs that is in the bottom 68 percent of all States historically receiving SBIR or STTR program funding.
(C) ESTABLISHMENT.—The Secretary of Defense shall establish a pilot program to provide small business concerns located in underperforming States an increased level of assistance under the SBIR and STTR programs of the Department.
(D) ACTIVITIES.—Under the pilot program, the Department, and any component agency thereof, may—
(A) in any case in which the Department seeks to make a Phase II SBIR or STTR award to a small business concern based on an application of a Phase I SBIR or STTR award to a small business concern by another agency, establish a streamlined transfer and fast track approval process for that Phase II award;
(B) provide an additional Phase II SBIR or STTR award to a small business concern...
located in an underperforming State that re-
ceived a Phase I SBIR or STTR award, sub-
ject to an increase in the allocation per-
centage.

(c) Establish a program to make Phase 1.5
SBIR or STTR awards to small business con-
cerns located in underperforming States in
order to provide funding for 12 to 24 months
to continue the development of technology; and

(d) Carry out subparagraph (c) along with other
mentorship programs.

(4) The pilot program established under this subsection shall terminate
5 years after the date on which the pilot pro-
gram is established.

(5) The Department shall submit to Congress an annual report on the sta-
tus of the pilot program established under this subsection, including the improvement in funding under the SBIR and STTR pro-
grams of the Department provided to small business concerns located in under-
performing States.''

SA 4802. Mr. OSSOFF (for himself, Mr. TILLIS, Mr. KING, Ms. CORTEZ
MASTO, Mr. ROUNDS, Mr. SCOTT of South Carolina, and Mr. KELLY) sub-
mitted an amendment intended to be
proposed to amendment SA 3867 sub-
mitted by Mr. REED and intended to be
proposed to the bill H.R. 4350, to au-
thorize appropriations for fiscal year
2022 for military activities of the De-
partment of Defense, for military con-
struction, 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 fol-
lowing:

SEC. ___. DR. DAVID SATCHEER CYBERSECURITY
EDUCATION GRANT PROGRAM.

(a) SHORT TITLE.—This section may be
cited as the “Cybersecurity Opportunity
Act”.

(b) DEFINITIONS.—In this section:

(1) DIRECTOR.—The term “Director” means
the Director of the National Institute of
Standards and Technology.

(2) ENROLLMENT OF NEEDY STUDENTS.—The term
“enrollment of needy students” has the
meaning given the term in section 312(d) of
the Higher Education Act of 1965 (20 U.S.C.
1058(d)).

(3) HISTORICALLY BLACK COLLEGE OR UNI-
VERSITY.—The term “historically Black college or
university” has the meaning given the term “part B institution” as defined in
section 322 of the Higher Education Act of

(4) INSTITUTION OF HIGHER EDUCATION.—The term
“institution of higher education” has the
meaning given the term in section 102(a)
1001(a)).

(5) MINORITY-SERVING INSTITUTION.—The term
“minority-serving institution” means an
institution listed in section 371(a) of
the Higher Education Act of 1965 (20 U.S.C.
1067q(a)).

(6) AUTHORIZATION OF GRANTS.—

(c) ESTABLISHMENT OF COMMISSION.—

(A) COMPOSITION.—The Commission shall
be composed of 16 members of whom—

(i) 1 shall be appointed by the Chairman
of the Committee on Armed Services of the
Senate;

(ii) 1 shall be appointed by the ranking
member of the Committee on Armed Serv-
ices of the Senate;

(iii) 1 shall be appointed by the Chairman
of the Committee on Armed Services of the
House of Representatives;

(iv) 1 shall be appointed by the ranking
member of the Committee on Armed Serv-
ices of the House of Representatives;

(b) REPORTING REQUIREMENTS.—Not later
than—

(1) 1 year after the effective date of this
section, as provided in subsection (h), and
annually thereafter until the Director sub-
mits the report under paragraph (2), the Di-
rector shall prepare and submit to Congress
a report on the status and progress of imple-
mentation of the grant programs under this
section, including on the number and nature of
institutions participating, the number and
nature of students served by institutions re-
ceiving grants, the level of funding provided
to grant recipients, the types of activities
being funded by the grants program, and
plans for future implementation and de-
velopment; and

(2) 5 years after the effective date of this
section, as provided in subsection (h), the Di-
rector shall prepare and submit to Congress
a report regarding the grant programs under
this section.

SEC. 1216. AFGHANISTAN WAR COMMISSION ACT
OF 2021.

(a) SHORT TITLE.—This section may be
cited as the “Afghanistan War Commission Act
of 2021”.

(b) DEFINITIONS.—In this section:

(1) APPLICABLE PERIOD.—The term “appli-
cable period” means the period beginning

(2) APPROPRIATE CONGRESSIONAL COMMIT-
TEES.—The term “appropriate congressional committees” means—

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

(B) the Committee on Armed Services of
the House of Representatives;

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

(D) the Committee on Appropriations of
the Senate;

(E) the Committee on Armed Services of
the House of Representatives;

(F) the Committee on Foreign Affairs of
the House of Representatives;

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

and

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

(3) INTELLIGENCE COMMUNITY.—The term
“intelligence community” has the meaning
given that term in section 3(4) of the Na-
tional Security Act of 1947 (50 U.S.C.
3003(4)).

(4) ESTABLISHMENT OF COMMISSION.—

(A) COMPOSITION.—The Commission shall
be composed of 16 members of whom—

(i) 1 shall be appointed by the Chairman
of the Committee on Armed Services of the
Senate;

(ii) 1 shall be appointed by the ranking
member of the Committee on Armed Serv-
ices of the Senate;

(iii) 1 shall be appointed by the Chairman
of the Committee on Armed Services of the
House of Representatives;

(iv) 1 shall be appointed by the ranking
member of the Committee on Armed Serv-
ices of the House of Representatives;
(v) 1 shall be appointed by the Chairman of the Committee on Foreign Relations of the Senate; (vi) 1 shall be appointed by the ranking member of the Committee on Foreign Relations of the Senate; (vii) 1 shall be appointed by the Chairman of the Committee on Foreign Affairs of the House of Representatives; (viii) 1 shall be appointed by the ranking member of the Committee on Foreign Affairs of the House of Representatives; (ix) 1 shall be appointed by the Chairman of the Select Committee on Intelligence of the Senate; (x) 1 shall be appointed by the ranking member of the Select Committee on Intelligence of the House of Representatives; (xi) 1 shall be appointed by the ranking member of the Permanent Select Committee on Intelligence of the House of Representatives; (xii) 1 shall be appointed by the majority leader of the Senate; (xiii) 1 shall be appointed by the minority leader of the Senate; (xiv) 1 shall be appointed by the Speaker of the House of Representatives; and (xv) 1 shall be appointed by the Majority Leader of the House of Representatives. (B) Qualifications.—It is the sense of Congress that each member of the Commission appointed under subparagraph (A) should have significant professional experience in national security, such as a position in—

(i) the Department of Defense; (ii) the Department of State; (iii) the intelligence community; (iv) the United States Agency for International Development; or

(v) an academic or scholarly institution. (C) Prohibitions.—A member of the Commission appointed under subparagraph (A) may not—

(i) be a current member of Congress; (ii) be a former member of Congress who served in Congress after January 3, 2001; (iii) be a current or former registrant under the Foreign Agents Registration Act of 1938 (22 U.S.C. 611 et seq.); (iv) have previously investigated Afghanistan, participated in the Afghanistan engagement through employment in the office of a relevant inspector general; (v) be a former owner or had a majority stake in a company that held any United States or coalition defense contract providing goods or services to activities by the United States Government or coalition in Afghanistan during the applicable period; or (vi) have served, with direct involvement in actions by the United States Government in Afghanistan during the time the relevant official served, as—

(I) a cabinet secretary or national security adviser to a President; or (II) a four-star flag officer, Under Secretary, or more senior official in the Department of Defense or the Department of State. (D) Date of Establishment.—(1) IN GENERAL.—The appointments of the members of the Commission shall be made not later than 60 days after the date of enactment of this Act. (2) FAILURE TO MAKE APPOINTMENT.—If an appointment under subparagraph (A) is not made by the appointment date specified in clause (1), the Co-Chairpersons of the Commission may submit an addendum to a report required under subclause (I) setting forth the progress of diplomatic, military, and intelligence efforts; (iii) the efficacy of interagency planning and execution process by the United States Government; (iv) factors that led to the collapse of the Afghan National Defense Security Forces in 2021, including—

(I) training; (II) assessment methodologies; (III) building indigenous forces on western model; (IV) reliance on technology and logistics support; and (V) reliance on warfare enablers provided by the United States. (v) the efficacy of counter-corruption efforts to include linkages to diplomatic lines of effort, linkages to foreign and security assistance, and assessment methodologies; (vi) the efficacy of counter-narcotic efforts to include alternative livelihoods, eradication, interdiction, and education efforts; (vii) the role of countries neighboring Afghanistan in contributing to the instability of Afghanistan; (viii) varying diplomatic approaches between Presidential administrations; (ix) the extent to which the intelligence community did or did not fail to provide sufficient warning about the probable outcomes of the withdrawal of coalition military support from Afghanistan, including as it relates to the capability and sustainability of the Afghan National Defense Security Forces; (ix) the sustainability of the Afghan central government, absent coalition support; (x) the extent of Taliban control over Afghanistan over time with respect to geographic territory, governance, and influence; and (x) the likelihood of the Taliban regaining control of Afghanistan at various levels of United States and coalition support, including the withdrawal of most or all United States or coalition support; (x) the extent to which intelligence products related to the state of the conflict in Afghanistan and the effectiveness of the Afghan National Defense Security Forces complied with intelligence community-wide analytic tradecraft standards and fully represented the diverse analytic views across the intelligence community; (xi) an evaluation of whether any element of the United States was provided with appropriately restricted access to data from elements of the intelligence community, Congress, or the Special Inspector General for Afghanistan Reconstruction (SIGAR) or any other oversight body such as other inspectors general or the Government Accountability Office, including through the use of overclassification; and (xii) the extent to which public representations of the situation in Afghanistan before Congress by United States Government officials were not consistent with the most recent formal assessment of the intelligence community at the time those representations were made. (2) REPORT REQUIRED.—(A) IN GENERAL.—(I) ANNUAL REPORT.—(I) IN GENERAL.—Not later than 1 year after the date of the initial meeting of the Commission, and annually thereafter, the Commission shall submit to the appropriate congressional committees a report describing the progress of the activities of the Commission as of the date of such report, including any findings, recommendations, or lessons learned endorsed by the Commission.
forth the separate views of such member with respect to any matter considered by the Commission.

(III) BRIEFING.—On the date of the submission of the annual report, the Commission shall brief Congress.

(ii) FINAL REPORT.—

(I) SUBMISSION.—Not later than 3 years after the date of the initial meeting of the Commission, the Commission shall submit to Congress a report that contains a detailed statement of the findings, recommendations, and lessons learned endorsed by the Commission.

(ii) ADDENDA.—Any member of the Commission, in accordance with subclause (I) setting forth the separate views of such member with respect to any matter considered by the Commission.

(iii) EXTENSION.—The Commission may submit the report required under subclause (I) at a date that is not more than 1 year later than the date specified in such clause if agreed to by the chairperson and ranking member of each of the appropriate congressional committees.

(B) FORMAL REPORT required by paragraph (1)(B) shall be submitted and publicly released on a Government website in unclassified form but may contain a classified annex.

(C) SUBSEQUENT REPORTS ON DECLASSIFICATION.—

(1) IN GENERAL.—Not later than 4 years after the date that the report required by subparagraph (A)(ii) is submitted, each relevant agency of jurisdiction shall submit to the committee of jurisdiction a report on the efforts of such agency to declassify such annex.

(ii) CONTENTS.—Each report required by clause (i) shall include the following:

(A) A list of the items in the classified annex that the agency is working to declassify at the time of the report and an estimate of the timeline for declassification of such items;

(B) A broad description of items in the annex that the agency is declining to declassify at the time of the report and an estimate of the timeline for declassification of such items;

(C) ANY JUSTIFICATION FOR WITHOLDING DECLASSIFICATION OF CERTAIN ITEMS IN THE ANNEX AND AN ESTIMATE OF THE TIMELINE FOR DECLASSIFICATION OF SUCH ITEMS;

(D) POWERS OF COMMISSION.—

(i) HEARINGS.—The Commission may hold such hearings as it deems necessary to receive such evidence as the Commission considers necessary to carry out its purpose and functions under this section.

(ii) ASSISTANCE FROM FEDERAL AGENCIES.—

(A) INFORMATION.—

(i) IN GENERAL.—The Commission may secure directly from a Federal department or agency such information as the Commission considers necessary to carry out this section.

(ii) FURNISHING INFORMATION.—Upon receipt of a written request by the Co-Chairpersons of the Commission, the head of the department or agency shall expeditiously furnish the information to the Commission.

(iii) SPACE FOR COMMISSION.—Not later than 30 days after the date of the enactment of this Act, the Administrator of General Services, in consultation with the Commission, shall identify and make available suitable excess space within the Federal space inventory to house the operations of the Commission. If the Administrator of General Services is not able to make such suitable excess space available within 30 days after the date of the enactment of this Act, the Commission may lease space to the extent that funds are available for such purpose.

(iv) POSTAL SERVICES.—The Commission may use the United States mails in the same manner and under the same conditions as other departments and agencies of the Federal Government.
2022 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 in title X, insert the following:

Subtitle — Veterans Matters

SEC. EXTENSIONS OF CERTAIN PROVISIONS OF LAW RELATING TO BENEFITS PROVIDED UNDER DEPARTMENT OF VETERANS AFFAIRS EDUCATIONAL ASSISTANCE PROGRAMS DURING COVID-19 PANDEMIC.

(a) Extension of Student Veterans Coronavirus Response Act of 2020.—Section 2 of the Student Veteran Coronavirus Response Act of 2020 (Public Law 116-146; 38 U.S.C. 3671 note), as amended by section 5202(a) of the Department of Veterans Affairs Expiring Authorities Act of 2020 (division E of Public Law 116-159), is further amended by striking “December 21, 2021” and inserting “June 1, 2022.”

(b) Extension of Payment of Work-Study Allowances During Emergency Situation.—Section 3 of the Student Veteran Coronavirus Response Act of 2020 (38 U.S.C. 3485 note) is amended by striking “During the covered period” and inserting “During the period beginning on March 1, 2020, and ending on December 21, 2021.”

(c) Extension of Period for Continuation of Department of Veterans Affairs Educational Assistance Benefits for Certain Programs of Education Converted to Distance Learning by Reason of Emergencies and Health-Related Situations.—Section 1(b) of Public Law 116-123 (38 U.S.C. 3601 note prev.), as amended by section 5202(b) of the Department of Veterans Affairs Expiring Authorities Act of 2020 (division E of Public Law 116-159), is further amended by striking “December 21, 2021” and inserting “June 1, 2022.”

(d) Extension of Modification of Time Limitations on Use of Entitlement to Montgomery GI Bill and Vocational Rehabilitation.—Section 1103(h) of such Act is amended by adding at the end the following new paragraph:

“(2) Paragraph (1) does not apply to the extension of the period of time for which the beneficiary may exercise the benefit under section 3333(g).”

(e) Extension of Continuation of Department of Veterans Affairs Educational Assistance Benefits During COVID-19 Emergency.—Section 1102(e) of the Johnny Isakson and David P. Roe, M.D. Veterans Health Care and Benefits Improvement Act of 2020 (Public Law 116-315) is amended by striking “December 21, 2021” and inserting “June 1, 2022.”

(f) Extension of Provisions Relating to extensions of closure of educational institution and modification of courses by reason of COVID-19 emergency.—Section 1103(b) of such Act is amended by striking “December 21, 2021” and inserting “June 1, 2022.”

(g) Extension of Provision Relating to Payment of Educational Assistance in Cases of Certain Emergencies.—Section 3694(a) of such Act is amended by striking “December 21, 2021” and inserting “June 1, 2022.”

(h) Extension of Provision Relating to Apprenticeship or On-Job Training Requirements.—Section 1106(b) of such Act is amended by striking “December 21, 2021” and inserting “June 1, 2022.”

(i) Extension of Provisions Relating to Verification of Enrollment for Certain Educational Institutions.—Section 3333(b) of title 38, United States Code, is amended by adding at the end the following new paragraph:

“(2) Waiver.—The Secretary may waive the requirements of this subsection for an educational institution the Secretary determines has used a flat tuition and fee structure that would make the use of a second verification under this subsection unnecessary.”

(j) Limitations on Authority to Disapprove of Courses.—(1) In General.—Subsection (f) of section 3679 of title 38, United States Code, is amended—

(A) in paragraph (2)(B),

(i) by inserting “, except for the recruitment of foreign students residing in foreign countries who are not eligible to receive Federal student assistance” after “assistance”;

and

(ii) by adding at the end the following new subparagraph:

“(C) by inserting ‘, except for the recruitment of foreign students residing in foreign countries who are not eligible to receive Federal student assistance’ after ‘assistance’.”

(k) Extension of Provision Relating to Enrollment of Foreign Students.—Section 3679 of title 38, United States Code, is amended by adding at the end the following new paragraph:

“(l) Waiver.—The Secretary may waive the requirements of this subsection for an educational institution the Secretary determines has used a flat tuition and fee structure that would make the use of a second verification under this subsection unnecessary.”

(l) Limitations on Authority to Disapprove of Courses.—(1) In General.—Subsection (f) of section 3679 of title 38, United States Code, is amended—

(A) in paragraph (2)(B),

(i) by inserting “, except for the recruitment of foreign students residing in foreign countries who are not eligible to receive Federal student assistance” after “assistance”;

and

(ii) by adding at the end the following new subparagraph:

“(C) by inserting ‘, except for the recruitment of foreign students residing in foreign countries who are not eligible to receive Federal student assistance’ after ‘assistance’.”

(m) Extension of Provision Relating to Assistance Available to Certain Covered Individuals.—Section 1094(a)(20) of the Higher Education Act of 1965 (20 U.S.C. 1094(a)(20)).

(n) Applicability Period.—Subsection (a) shall apply during the period beginning on December 21, 2021, and ending on June 1, 2022.

(o) Definitions.—In this section:

(1) Educational institution.—The term ‘educational institution’ has the meaning given that term in section 3621 of title 38, United States Code, and includes an institution of higher learning (as defined in such section).

(2) Program of education.—The term ‘program of education’ means the term ‘education program’ as defined in section 498(a)(20) of the Higher Education Act of 1965 (20 U.S.C. 1094(a)(20)).

(p) Budgetary Effects.—There shall be offset against any other appropriation for veterans affairs for such fiscal year for veterans affairs for—

(1) the amount described in section 3686(c) of title 38, United States Code, and

(2) the amount described in section 3686(d) of title 38, United States Code.

SEC. MODIFICATIONS TO REQUIREMENTS FOR EDUCATIONAL INSTITUTIONS PARTICIPATING IN THE EDUCATIONAL ASSISTANCE PROGRAMS OF THE DEPARTMENT OF VETERANS AFFAIRS.

(a) Waiver or Verification of Enrollment for Certain Educational Institutions.—(1) Section 3333(b) of title 38, United States Code, is amended by adding at the end the following new paragraph:

“(2) Waiver.—The Secretary may waive the requirements of this subsection for an educational institution the Secretary determines has used a flat tuition and fee structure that would make the use of a second verification under this subsection unnecessary.”

(b) Limitations on Authority to Disapprove of Courses.—(1) In General.—Subsection (f) of section 3679 of title 38, United States Code, is amended—

(A) in paragraph (2)(B),

(i) by inserting “, except for the recruitment of foreign students residing in foreign countries who are not eligible to receive Federal student assistance” after “assistance”;

and

(ii) by adding at the end the following new subparagraph:

“(C) by inserting ‘, except for the recruitment of foreign students residing in foreign countries who are not eligible to receive Federal student assistance’ after ‘assistance’.”

(c) Extension of Foreign Schools From Certain Requirements.—(1) Information Relating to Tests.—Section 3686(c) of title 38, United States Code, is amended by adding at the end the following new paragraph:

“(3) Subparagraph (G) of paragraph (1) shall not apply with respect to an educational institution located in a foreign country.”

(2) Examination of Records.—Section 3690(c) of title 38, United States Code, is amended—

(A) by striking “Notwithstanding” and inserting “(1) Except as provided in paragraph (2), notwithstanding’’; and

(B) by adding at the end the following new paragraph:

“(2) Paragraph (1) does not apply to the records and accounts—

(A) of an educational institution located in a foreign country; and

(B) that pertain to an individual who is not receiving educational assistance under this chapter.”

SEC. CONTINUATION OF DEPARTMENT OF VETERANS AFFAIRS EDUCATIONAL ASSISTANCE PROGRAMS FOR CERTAIN PROGRAMS OF EDUCATION CONVERTED TO DISTANCE LEARNING BY REASON OF EMERGENCIES AND HEALTH-RELATED SITUATIONS.

(a) In General.—In the case of a program of education approved by a State approving agency, or the Secretary of Veterans Affairs when acting in the role of a State approving agency, that is converted from being offered only at an educational institution being offered by distance learning by reason of an emergency or health-related situation, as determined by the Secretary, the Secretary may continue to offer assistance under the laws administered by the Secretary without regard to such conversion, including with respect to paying any—

(1) monthly housing stipends under chapter 33 of title 38, United States Code; or

(2) payments or subsistence allowances under chapters 30, 31, 32, and 35 of such title and chapters 1606 and 1607 of title 10, United States Code.

(b) Applicability Period.—Subsection (a) shall apply during the period beginning on December 21, 2021, and ending on June 1, 2022.

(c) Definitions.—In this section:

(1) Educational institution.—The term ‘educational institution’ has the meaning given that term in section 3602 of title 38, United States Code, and includes an institution of higher learning (as defined in such section).

(2) Program of education.—The term ‘program of education’ has the meaning given that term in section 3302 of title 38, United States Code.

(3) State approving agency.—The term ‘State approving agency’ has the meaning given that term in section 3671 of title 38, United States Code.

SEC. BUDGETARY EFFECTS.

(a) In General.—Amounts provided to carry out the amendments made by this subtitle are designated as an emergency requirement pursuant to section 6302 of title 31, United States Code, and shall be considered for the purpose of carrying out this subtitle.

(b) Designation in Senate.—In the Senate, amounts provided to carry out the amendments made by this subtitle are designated as an emergency requirement pursuant to section 412(a) of H. Con. Res. 71 (115th Cong.), the concurrent resolution on the budget for fiscal year 2018.

SA 4806. Ms. SMITH (for herself and Mr. YOUNG) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense; defense health care and medical construction, and for defense activities of the Department of Energy, to prescribe military personnel
The term "One Health" reflects the interconnectedness of human health, animal health, and the environment. As technology and population growth facilitates increased interaction of human settlements with wildlife habitats and as international travel and trade increases, the interface between these elements will also continue to rise.

(2) When zoonotic diseases spill over to humans, there are often enormous health and economic costs. The World Bank estimates that, between 1997 and 2006, the global costs from six zoonotic outbreaks exceeded $300,000,000,000 and the Centers for Disease Control and Prevention estimates that there are annually 2,500,000,000 cases of zoonotic infections globally, resulting in 2,700,000 deaths.

(3) There are also immense effects on the agriculture sector. In 2014 and 2015, a high pathogenic avian influenza (HPAI) outbreak in the United States led to the cull of nearly 50,000,000 birds, and imposed up to approximately 62,300,000,000 in losses for poultry and egg farmers, animal feed producers, baked good production, and other related industries.

(4) Public health preparedness depends on agriculture in a variety of ways. For example, a wide range of vaccines, including those for influenza, yellow fever, rabies, and measles—mumps—rubella (MMR), are primarily cultivated in poultry eggs. Egg shortages resulting from zoonotic disease outbreaks could impose serious risks to vaccine manufacturing efforts.

(5) It is estimated that approximately 80 percent of potential pathogens likely to be used in bioterrorism or biowarfare are common zoonotic pathogens.

(6) While existing Federal Government initiatives related to One Health span multiple agencies, including the Centers for Disease Control and Prevention, the Department of Homeland Security, the Department of Agriculture Animal and Plant Health Inspection Services’ One Health Coordination Center, the Department of Energy, the National Institutes of Health, the Department of the Interior, the Centers for Disease Control and Prevention, and the Department of Labor, the One Health Framework (referred to in this title as the ‘‘framework’’) for coordinated Federal activities under the One Health Program.

The framework will (1) shall describe existing efforts and contain recommendations for building upon and complementing the activities of the Department of State and the Department of Homeland Security, the Department of the Interior, the Centers for Disease Control and Prevention, the Food and Drug Administration, the Office of the Assistant Secretary for Preparedness and Response, the Department of Agriculture, the United States Agency for International Development, the Environmental Protection Agency, the National Institutes of Health, the Department of Homeland Security, and other departments and agencies to prevent and respond to zoonotic disease outbreaks in animals and humans; and

(2) contains an evaluation of the framework and the specific activities requested to achieve the framework.

SEC. 1064. STUDY AND REPORT ON THE REDISTRIBUTION OF COVID–19 VACCINE DOSES THAT WOULD OTHERWISE EXPIRE TO FOREIGN COUNTRIES AND ECONOMIES.

(a) STUDY.—(1) IN GENERAL.—The Secretary of Health and Human Services, in consultation with the Secretary of State and the Administrator of the United States Agency for International Development, shall conduct a study to identify and analyze the logistical pre-requisites for the collection of unused and expired doses of the COVID–19 vaccine in the United States and for the distribution of such doses to foreign countries and economies.

(b) MATTERS STUDIED.—The matters studied by the Secretary of Health and Human Services under paragraph (1) shall include—

(A) options for the collection of unused and expired doses of the COVID–19 vaccine from entities in the United States;

(B) methods for the collection and shipment of such doses to foreign countries and economies;

(C) methods for ensuring the appropriate storage and handling of such doses during and following the distribution and delivery of the doses to such countries and economies;

(D) the capacity and capability of foreign countries and economies receiving such doses to store and handle the doses while assuring their safety and quality;

(E) the minimum supply of doses of the COVID–19 vaccine necessary to be retained within the United States; and

(F) other Federal agencies with which the heads of the relevant agencies should coordinate to accomplish the tasks described in paragraphs (A) through (E) and the degree of coordination necessary between such agencies.
SA 4808. Mrs. FEINSTEIN (for herself, Mrs. Ernst, Mr. Durbin, Ms. Colins, Ms. Rosen, Ms. Blumenthal, Ms. Peters, Mr. Cornyn, and Ms. Duckworth) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. Reed and intended to be proposed to the bill H.R. 4300, to authorize appropriations for fiscal year 2022 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. The amendment is as follows:

At the end of subtitle B of title XII, add the following:

SEC. 1216. STATUS OF WOMEN AND GIRLS IN AFGHANISTAN.

(a) FINDINGS.—Congress finds the following:

(1) Since May 2021, the escalation of violent conflict in Afghanistan has displaced an estimated 655,000 civilians, and 80 percent of those forced to flee are women and children.

(2) Since reining control of Afghanistan in August 2021, the Taliban have taken actions reminiscent of their brutal rule in the late 1990s, including by cracking down on protests and beating journalists, re-establishing the Ministry for the Promotion of Virtue and Prevention of Vice, and requiring women to study at universities in gender-segregated classrooms while wearing Islamic attire.

(3) Until the Taliban assumed control of the country in August 2021, the women and girls in Afghanistan achieved notable gains, including access to education, the right to vote, and women’s representation in government. However, the Taliban’s return to power has reversed these gains, placing an estimated 655,000 civilians, and 80 percent of those forced to flee are women and children.

(4) In Afghanistan, the high prevalence of anemia among adolescent girls reduces their ability to survive childbirth, especially when coupled with lack of access to safe abortion.

(b) STRATEGIC CONSIDERATIONS.—It is the sense of Congress that:

(1) since 2001, organizations and networks promoting the empowerment of women and girls have been important engines of social, economic, and political development in Afghanistan;

(2) any future political order in Afghanistan should secure the political, economic, and social gains made by Afghan women and work to increase the equal treatment of women and girls;

(3) respecting the internationally recognized human rights of all people is essential to ensuring lasting peace and sustainable development in Afghanistan;

(4) in consultation with international partners, the United States must endeavor to preserve the hard-won gains made in Afghanistan during the past two decades, particularly as related to the social, economic and political empowerment of women and girls in society.

(c) POLICY OF THE UNITED STATES REGARDING THE RIGHTS OF WOMEN AND GIRLS IN AFGHANISTAN.—

(1) IN GENERAL.—It is the policy of the United States—

(A) to continue to support the internationally recognized human rights of women and girls in Afghanistan following the withdrawal of the United States Armed Forces from Afghanistan, including through mechanisms to hold to account those publicly accountable for violations of international humanitarian law and violations of such rights against women and girls;

(B) to continue to support the internationally recognized political and economic rights of women and girls in Afghanistan;

(C) to protect and promote the participation of women and girls in Afghanisms and those women and girls may again face the intimidation and marginalization they faced under the last Taliban regime.

(d) LEADERSHIP OF THE UNITED STATES.—

(1) The President shall—

(A) An assessment of the political and economic rights of women and girls in Afghanistan;

(B) to strongly oppose any weakening of internationally recognized human rights of women and girls in Afghanistan, including the right to safe work;

(C) to continue to support the internationally recognized political and economic rights of women and girls in Afghanistan;

(D) to systematically consult with Afghan women and girls on their needs and priorities in the development, implementation, and monitoring of human rights action, including women and girls who are part of the Afghan diaspora community.

(e) REPORT ON WOMEN AND GIRLS IN AFGHANISTAN.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and every 180 days thereafter through 2024, the Secretary of State shall submit to the appropriate committees of Congress, and make available to the public, a report that includes the following:

(A) an assessment of the status of women and girls in Afghanistan following the departure of United States and partner military forces, including with respect to access to primary and secondary education, jobs, primary and emergency health care, and legal protections and status.

(B) An assessment of the political and civic participation of women and girls in Afghanis—

(C) An assessment of the prevalence of gender-based violence in Afghanistan,

(d) HUMANITARIAN ASSISTANCE AND AFGHAN WOMEN.—The Administrator of the United States Agency for International Development should work to ensure that Afghan women employed and enabled to work in the delivery of humanitarian assistance in Afghanistan, to the extent practicable.

(e) REPORT ON WOMEN AND GIRLS IN AFGHANISTAN.—
gender equality and the internationally rec-
ognized human rights of women and girls in
Afghanistan, including funds directed toward
local organizations promoting such rights of
women and girls, and (ii) includes the follow-
ing:
(i) The amounts awarded to principal re-
cipients and sub-recipients for such purposes
during the reporting period;
(ii) A description of each program for
which such funds are used for such purposes.
SA 4809. Mr. WARNER submitted an
amendment intended to be proposed to
amendment SA 3867 submitted by Mr. REED to
the bill H.R. 4350, to authorize appro-
priations for fiscal year 2022 for mili-
tary activities of the Department of
Defense, for military construction, and
for defense activities of the Depart-
ment 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:
SEC. 576. COUNTERING EXTREMISM IN THE
ARMED FORCES.
(a) In General.—The Secretary of Defense
shall—
(1) promulgate policy that prohibits and
defines participation in extremist activities;
(2) develop and implement programs,
resources, and activities to counter extremism
within the Armed Forces, including screen-
ing of publicly available information and
Insider Threat Programs;
(3) collect and report data on incidents, al-
elgations, investigations, disciplinary ac-
tions, and separations related to extremism,
as well as publication of reports on these
data in a regular, public, and transparent
manner; and
(4) designate a senior official, to be known as
the "Senior Official for Countering Extrem-
ism in the Armed Forces" (in this subsection
defined as the "Office") to be responsible for
facilitating and coordination of
the activities described in this subsection
with personnel and readiness officials, law
enforcement organizations, security organi-
zations, insider threat programs, and watch
lists related to extremism in the Armed
Forces.
(b) TRAINING AND EDUCATION.—
(1) In General.—The Secretary of each
military department, in coordination with
the Senior Official for Countering Extrem-
ism in the Armed Forces, shall develop and
implement training and education programs and related
materials to assist members of the Armed Forces
and civilian employees of the Department of
Defense in identifying, preventing, respond-
ing to, reporting, and mitigating the risk of
extremist activities.
SEC. 577. ESTABLISHMENT OF STRUCTURE
AND AUTHORITIES TO ADDRESS UN-
IDENTIFIED AERIAL PHENOMENA.
(a) ESTABLISHMENT OF ANOMALY
SURVEILLANCE, TRACKING, AND RESOLUTION
OFFICE.—
(1) In General.—Not later than 180 days
after the date of the enactment of this
Act, the Secretary of Defense shall, in coordi-
nation with the Director of National Intel-
ligence, establish an office within an appro-
priate component of the Department of
Defense, to be known as the Anomaly
Surveillance, Tracking, and Resolution
Office (in this section referred to as the
"Office") to—
(A) develop procedures to synchronize
the Unidentified Aerial Phenomenon
Task Force or subordinate it to the Office.
(b) FACILITATION OF REPORTING AND DATA
SHARING.—The Director and the Secretary
shall, in coordination with each other, require that—
(1) each element of the intelligence com-
munity and the Department, with any data
available adequate personnel with requisite
expertise, equipment, transportation, and other
resources necessary to respond rapidly to
incidents or patterns of observations of
unidentified aerial phenomena, make such
data available immediately to the Office; and
(2) military and civilian personnel em-
ployed by or under contract to the Depart-
ment or an element of the intelligence
community shall have access to procedures
by which incidents involving unidentified aerial phenomena
are reported, as described in subsection
(b).
(c) DUTIES.—The duties of the Office estab-
lished under subsection (a) shall include the
following:
(1) Developing procedures to synchronize
and standardize the collection, reporting,
and analysis of incidents, including adverse
physiological effects, regarding unidentified
aerial phenomena across the Department and
the intelligence community.
(2) Developing processes and procedures
to ensure that such incidents from each compo-
nent of the Department and the intelligence
community are reported and incorporated in a centralized
repository.
(3) Developing procedures to require the
timely and consistent reporting of such inci-
dents.
(4) Evaluating links between unidentified
aerial phenomena and adversarial foreign
government organizations, other foreign governments,
or nonstate actors.
(5) Evaluating the threat that such inci-
dents present to the United States.
(c) DUTIES.—The Office shall—
(1) in coordination with other departments
and agencies of the Federal Government, as
appropriate, including the Federal Aviation
Administration, the National Aeronautics
and Space Administration, the Department
of Homeland Security, the National Oceanic
and Atmospheric Administration, and the
Department of Energy,
consulting with allies and partners of the
United States, as appropriate, to better
assess the nature and extent of unidentified
aerial phenomena;
(2) preparing reports for Congress, in both
classified and unclassified form, as required
by subsections (b) and (i).
(c) Employment of Line Organizations for
Field Investigations of Unidentified Aerial
Phenomena.—
(1) In General.—The Secretary shall, in
coordination with the Director, designate line
organizations within the Department of
Defense and the intelligence community
that possess appropriate expertise, authorities,
accesses, data, systems, platforms, and capa-
bilities to rapidly respond to, and conduct
field investigations of, incidents involving
unidentified aerial phenomena under the di-
rection of the Office.
(c) PERSONNEL, EQUIPMENT, AND RESOURCES.—The Secretary, in coordination
with the Director, shall take such actions as
may be necessary to ensure that the des-
ignated organization or organizations have
available adequate personnel with requisite
expertise, equipment, transportation, and
other resources necessary to respond rapidly
to incidents or patterns of observations of
unidentified aerial phenomena of which the
Office becomes aware.
(d) Utilization of Line Organizations for
Strategic, Operational, and Technical Analyses of
Data on Unidentified Aerial Phenomena.—
(1) IN GENERAL.—The Secretary, in coordination with the Director, shall designate one or more line organizations that will be primarily responsible for scientific, technical, and operational analysis of data gathered from field investigations conducted under subsection (d), or data from other sources, including testing of materials, medical studies, and development of theoretical models to better understand and explain unidentified aerial phenomena.

(2) AUTHORITY.—The Secretary and the Director on recommendation of such line organizations necessary to ensure that the designated line organizations have authority to draw on expertise of persons outside the Federal Government with appropriate security clearances.

(3) INTELLIGENCE COLLECTION AND ANALYSIS PLAN.—

(i) In general.—The head of the Office shall supervise the development and execution of an intelligence collection and analysis plan on behalf of the Secretary and the Director to gain as much knowledge as possible regarding the technical and operational characteristics, origins, and intentions of unidentified aerial phenomena, including the development, acquisition, deployment, and operation of technical collection capabilities necessary to detect, identify, and scientifically characterize unidentified aerial phenomena.

(ii) Use of resources and capabilities.—In developing the plan required by paragraph (1), the Office shall consider and propose, as appropriate, the use of any resource, capability, asset, or process of the Department and the intelligence community.

(iii) Science plan.—The head of the Office shall supervise the development and execution of a science plan on behalf of the Secretary to develop, to the extent practicable, scientific theories to account for the characteristics and performance of unidentified aerial phenomena that exceed the known state of the art in science or technology, including in the areas of propulsion, aerodynamic control, signatures, structures, materials, sensors, countermeasures, weapons, electronics, and power generation, and to provide the foundation for potential future investments to replicate any such advances and performance.

(iv) Assignment of priority.—The Director, in consultation with, and with the recommendation of the Secretary, shall assign an appropriate priority within the National Intelligence Priorities Framework to the requirement to understand, characterize, and respond to unidentified aerial phenomena.

(v) Authorization of appropriations.—There is authorized to be appropriated such sums as may be necessary to carry out the work of the Office, including—

(A) General intelligence gathering and intelligence analysis; and

(B) Military, defense, space defense, defense of controlled air space, defense of ground, air, or naval assets, and related purposes.

(4) ANNUAL REPORT.—

(A) In general.—Not later than January 31, 2022, and annually thereafter until October 31, 2026, the Secretary in consultation with the Director, shall submit to the appropriate committee of Congress a report on unidentified aerial phenomena.

(B) Elements.—Each report pursuant to paragraph (1) shall include, with respect to the year covered by the report, the following information:

(i) An analysis of data and intelligence received through reports of unidentified aerial phenomena.

(ii) An analysis of data relating to unidentified aerial phenomena collected through —

(A) Geospatial intelligence; and

(B) Signals intelligence.

(5) SUBSEQUENT BRIEFIGINGS.—Each briefing provided subsequent to the first briefing described in paragraph (2) shall include, at a minimum, all events relating to unidentified aerial phenomena that occurred during the previous 180 days, and events relating to unidentified aerial phenomena that were not included in an earlier briefing due to delay or consideration of the reporting system or other such factors.

(6) INSTANCES IN WHICH DATA WAS NOT SHARED.—For each briefing period, the Chair and Vice Chair of the Select Committee on Intelligence of the Senate, the Chair and Vice Chair of the Select Committee on Intelligence of the House of Representatives, shall receive an enumeration of any instances in which data related to unidentified aerial phenomena was denied to the Office because of classification restrictions on that data or for any other reason.

(1) AERIAL AND TRANSMEDIUM PHENOMENA ADVISORY COMMITTEE.—

(A) Establishment.—(A) Not later than October 1, 2022, the Secretary and the Director shall establish an advisory committee for the purpose of—

(i) Advising the Secretary in the execution of the duties of the Office as provided by this subsection; and

(ii) Advising the Secretary and the Director regarding the gathering and analysis of data, technical and scientific research and development, and scientific and technological assessments pertaining to unidentified aerial phenomena.

(B) Membership.—(A) Subject to subparagraph (B), the Committee shall be composed of members as follows:

(1) Twenty members selected by the Secretary as follows:

(A) Three members selected from among individuals recommended by the Administrator of the National Aeronautics and Space Administration.

(B) Ten members selected from among individuals recommended by the President of the American Society for Photogrammetry and Remote Sensing.

(C) Ten members selected from among individuals recommended by the President of the Optical Technology Center at Montana State University.

(D) Two members selected from among individuals recommended by the President of the American Institute of Astronautics and Aeronautics.

(E) Two members selected from among individuals recommended by the Director of the Galileo Project at Harvard University.

(F) Two members selected from among individuals recommended by the Administrator of the National Nuclear Security Administration.

(G) Two members selected from among individuals recommended by the President of the National Academy of Engineering.

(H) Two members selected from among individuals recommended by the President of the Optical Technology Center at Montana State University.

(I) One member selected from among individuals recommended by the President of the National Academy of Science.

(2) Five members selected from among individuals recommended by the President of the American Academy of Arts and Sciences.

(B) In general.—The President shall, from time to time, increase or decrease the size of the Committee, except that the size of the Committee shall not be more than 50 members.

(2) SEMIANNUAL BRIEFIGINGS.—

(A) In general.—Not later than 90 days after the date of the enactment of this Act and not less frequently than semiaannually thereafter, the Secretary, in consultation with the Director, shall provide the classified briefings on unidentified aerial phenomena to—

(i) The Committee on Armed Services, the Select Committee on Intelligence, and the Committee on Appropriations of the Senate; and

(ii) The Committee on Armed Services, the Permanent Select Committee on Intelligence, and the Committee on Appropriations of the House of Representatives.

(B) Upon request.—The briefings provided under paragraph (1) shall include all incidents involving unidentified aerial phenomena that were reported to the United States Government under subsection (a) during the period from January 1, 2021, to the date of occurrence of the incident.

(3) SUBSEQUENT BRIEFIGINGS.—Each briefing provided subsequent to the first briefing described in paragraph (2) shall include, at a minimum, all events relating to unidentified aerial phenomena that occurred during the previous 180 days, and events relating to unidentified aerial phenomena that were not included in an earlier briefing due to delay or consideration of the reporting system or other such factors.

(4) INSTANCES IN WHICH DATA WAS NOT SHARED.—For each briefing period, the Chair and Vice Chair of the Select Committee on Intelligence of the Senate, and the Chair and Vice Chair of the Select Committee on Intelligence of the House of Representatives shall receive an enumeration of any instances in which data related to unidentified aerial phenomena was denied to the Office because of classification restrictions on that data or for any other reason.

(1) AERIAL AND TRANSMEDIUM PHENOMENA ADVISORY COMMITTEE.—

(A) Establishment.—(A) Not later than October 1, 2022, the Secretary and the Director shall establish an advisory committee for the purpose of—

(1) Advising the Secretary in the execution of the duties of the Office as provided by this subsection; and

(2) Advising the Secretary and the Director regarding the gathering and analysis of data, technical and scientific research and development, and scientific and technological assessments pertaining to unidentified aerial phenomena.

(B) Membership.—(A) Subject to subparagraph (B), the Committee shall be composed of members as follows:

(1) Twenty members selected by the Secretary as follows:

(A) Three members selected from among individuals recommended by the Administrator of the National Aeronautics and Space Administration.

(B) Ten members selected from among individuals recommended by the American Society for Photogrammetry and Remote Sensing.

(C) Ten members selected from among individuals recommended by the President of the Optical Technology Center at Montana State University.

(D) One member selected from among individuals recommended by the President of the American Academy of Arts and Sciences.

(E) Five members selected from among individuals recommended by the President of the Optical Technology Center at Montana State University.

(F) One member selected from among individuals recommended by the President of the American Society for Photogrammetry and Remote Sensing.

(B) In general.—The President shall, from time to time, increase or decrease the size of the Committee, except that the size of the Committee shall not be more than 50 members.

(2) SEMIANNUAL BRIEFIGINGS.—

(A) In general.—Not later than 90 days after the date of the enactment of this Act and not less frequently than semiaannually thereafter, the Secretary, in consultation with the Director, shall provide the classified briefings on unidentified aerial phenomena to—

(i) The Committee on Armed Services, the Select Committee on Intelligence, and the Committee on Appropriations of the Senate; and

(ii) The Committee on Armed Services, the Permanent Select Committee on Intelligence, and the Committee on Appropriations of the House of Representatives.

(B) Upon request.—The briefings provided under paragraph (1) shall include all incidents involving unidentified aerial phenomena that were reported to the United States Government under subsection (a) during the period from January 1, 2021, to the date of occurrence of the incident.
(A) The Committee shall elect a Chairperson from among its members, who will serve a term of 2 years, and is eligible for re-election.

(4) Expert assistance, advice, and recommendations. The Committee may, upon invitation of the head of the Office, provide expert assistance or advice to any line organization designated to carry out field investigations or data analysis as authorized by subsections (d) and (e).

(B) The Committee, on its own initiative, or at the request of the Director, the Secretary, or the head of the Office, may provide advice and recommendations regarding best practices with respect to the gathering and analysis of data on unidentified aerial phenomena, including specific incidents, cases, or classes of unidentified aerial phenomena.

(5) Report. Not later than December 31, 2022, and not later than December 31 of each year thereafter, the Committee shall submit a report summarizing its activities and recommendations to the following:

(A) The Secretary
(B) The Director
(C) The head of the Office
(D) The Committee on Armed Services, the Select Committee on Intelligence, and the Committee on Appropriations of the Senate.
(E) The Committee on Armed Services, the Permanent Select Committee on Intelligence, and the Committee on Appropriations of the House of Representatives.

(6) Relation to FACA. For purposes of this subsection, the term "advisory committee" shall be defined to mean any committee, commission, or subcommittee established by an advisory committee (as defined in section 3 of the Federal Advisory Committee Act (5 U.S.C. 3003)).

(7) Termination of Committee. The Committee shall terminate on the date that is six years after the date of the establishment of the Committee.

(m) Definitions. In this section:

(1) The term "appropriate committees of Congress" means—

(A) the Committee on Armed Services, the Select Committee on Intelligence, the Committee on Foreign Relations, and the Committee on Appropriations of the Senate; and
(B) the Committee on Armed Services, the Permanent Select Committee on Intelligence, the Select Committee on Appropriations of the Senate; and
(C) the Committee on Armed Services, the Permanent Select Committee on Intelligence, and the Committee on Appropriations of the House of Representatives.

(2) The term "intelligence community" has the meaning given such term in section 3 of the National Security Act of 1947 (50 U.S.C. 1030).

(3) The term "transmedium objects or devices" means objects or devices that are observed to transition between space and the atmosphere, or between the atmosphere and bodies of water, that are not immediately identifiable.

(4) The term "unidentified aerial phenomena" means—

(A) airborne objects that are not immediately identifiable;

(B) transmedium objects or devices;

(C) submerged objects or devices that are not immediately identifiable and that display behavior or performance characteristics suggesting that they may be related to the subjects described in subparagraph (A) or (B).

EC. PROHIBITING THE INTERNAL REVENUE SERVICE FROM REQUIRING FINANCIAL INSTITUTIONS TO REPORT CUSTOMERS’ FINANCIAL ACCOUNT INFORMATION REPORTING PROGRAMS.

(a) FINDINGS. Congress finds the following:

(1) The Thrift Savings Fund invests more than $6,000,000,000 on behalf of participants. As the guardian of the retirement funds of approximately 6,000,000 Federal civil and military plan participants, it is critical that sums in the Thrift Savings Fund are not invested in securities linked to the economy of the People’s Republic of China.

(2) Companies headquartered in the People’s Republic of China have repeatedly committed corporate espionage, violated sanctions imposed by the United States, flouted international property laws, committed theft, and failed to comply with audit and regulatory standards designed to safeguard investors.

(3) The Thrift Savings Plan is known for its low management fees and comprehensive array of investment strategies. The provisions of this section, and the amendments made by this section, will not increase fees imposed on participants of the Thrift Savings Plan.

(4) The November 2019 vote of theMSCI ACWI Index by the Federal Retirement Thrift Investment Board, initially scheduled to be effective in 2020, would violate the terms of subsection (i) of section 8438 of title 5, United States Code, as added by subsection (b)(1) of this section.

(b) PROHIBITION ON TSP FUND INVESTMENT IN ENTITIES BASED IN THE PEOPLE’S REPUBLIC OF CHINA.—

(1) In General. Section 8438 of title 5, United States Code, is amended by adding at the end the following:

"(1) Notwithstanding any other provision of this section, no fund established or over-

seen by the Board may include an invest-
mixed in any security of—

(i) an entity based in the People’s Republic of China;

or

(ii) a subsidiary that is owned or oper-

ated by a parent entity described in sub-
paragraph (i); or

or

(ii) any subsidiary that is owned or oper-

ated by an entity that is described in sub-
paragraph (i)."

(2) Divestiture of Assets. Not later than 30 days after the date of enactment of this Act, the Federal Retirement Thrift Investment Board established under section 8472(a) of title 5, United States Code, shall—

(A) review whether any sums in the Thrift Savings Fund are invested in violation of subsection (i) of section 8438 of that title, as added by paragraph (1) of this subsection;

(B) if any sums are invested in the manner described in subparagraph (A), divest those sums in a manner that is consistent with the legal and fiduciary duties provided under chapter 84 of that title, or any other applica-
tive provision of law; and

(C) reinvest any sums divested under sub-

paragraph (B) in investments that do not violate subsection (i) of section 8438 of that title, as added by paragraph (1) of this subsection.

(c) PROHIBITION ON INVESTMENT OF TSP FUNDS IN ENTITIES BASED IN THE PEOPLE’S REPUBLIC OF CHINA THROUGH THE TSP MUTUAL FUND WINDOW.—Section 8438(b)(5) of title 5, United States Code, is amended by adding at the end the following:

"(E) A mutual fund accessible through a mutual fund window authorized under this
tion Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)).

"(3) COVERED CYBER INCIDENT.—The term ‘covered cyber incident’ means a substantial cyber incident or group of those incidents that together satisfy such definition, consisting of ransom payments, particularly with respect to ongoing cyber threats or security vulnerabilities and identity and disseminate ways to prevent or mitigate similar incidents in the future;

"(7) for a covered cyber incident, including a ransomware attack, that also satisfies the definition of a significant cyber incident, or is part of a group of related cyber incidents that together satisfy such definition, conducted in coordination with those covered cyber incident or group of those incidents and identity and disseminate ways to prevent or mitigate similar incidents in the future;

"(8) with respect to covered cyber incident reports under section 2232(a) and 2233 involving ongoing cyber threats or security vulnerabili,

immediately review those reports for cyber threat indicators that can be anonymized and disseminated, with defen

and incident response firms, and security research

cidents in the future; in coordination with other divisions withi

the Agency, as appropriate;

publish quarterly unclassified, public reports that may be released as the unclassified information contained in the briefings required under subsection (c);

proactively identify opportunities and perform analyses, consistent with the protections in section 2235, to leverage and utilize data on ransomware attacks to support law enforcement investigations to identify, track, and seize ransom payments, virtual currencies, to the greatest extent practicable;

proactively identify opportunities, consistent with the protections in section 2235, to leverage and utilize data on cyber incidents in a manner that enables and strengthens cybersecurity research carried out by private sector organizations, to the greatest extent practicable; and

themselves on one or more of:

for protection of the confidence, national securi

ties, foreign relations, or economy of the United

财政年，和对其他目的; and

fiscal year, and for other purposes; and

of the Homeland Security Act of 2002 (6 U.S.C. 1501 et seq.) reports from covered entities (as defined in section 2230) submitted by covered entities (as defined in section 2230) and reports related to ransom payments submitted by entities in furtherance of the activities specified in sections 2202(e), 2203, and 2231, this subsection, and any other authorized activity of the Director, to enhance the situational awareness of cybersecurity threats across critical infrastructure sectors.; and (2) by adding at the end the following:

"Subtitle C—Cyber Incident Reporting

"SEC. 2230. DEFINITIONS.

In this subtitle:

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

"(2) COUNCIL.—The term ‘Council’ means the Cyber Incident Review Center created in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Au

"public health and safety, and to have a more accurate picture of the cyber threat to critical infrastructure and the people of the United States;

"(11) receive, aggregate, analyze, and secure reports to lead the identification of tactics, techniques, and procedures used to perpetrate cyber incidents and ransomware at;

"(4) leverage information gathered about cybersecurity incidents to—

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

"(9) for a covered cyber incident, as defined in subsection (a), that is below the micro-purchase threshold, does not include any activity related to good faith security research, including participation in a bug-bounty program or a vulnerability disclosure program.

"(7) FEDERAL CONTRACTOR.—The term ‘Federal contractor’ means a business, nonprofit organization, or entity that holds a Federal Government contract or subcontract at any tier, grand, cooperative agreement, or other transaction agreement, unless that entity is a party only—

"(A) a service contract to provide housekeeping or custodial services;

"(B) a contract to provide products or services unrelated to information technology that is below the micro-purchase threshold, as defined in section 2.101 of title 48, Code of Federal Regulations, or any successor regulation.

"(4) COVERED ENTITY.—The term ‘covered entity’ means—

"(A) any Federal contractor;

"(B) an entity that owns or operates critical infrastructure that satisfies the definition established by the Director in the final rule issued pursuant to section 2232(b).

"(4) COVERED ENTITY.—The term ‘covered entity’ means—

"(A) any Federal contractor; or

"(B) an entity that owns or operates critical infrastructure that satisfies the definition established by the Director in the final rule issued pursuant to section 2232(b).

"(5) CYBER INCIDENT.—The term ‘cyber incident’ has the meaning given the term ‘incident’ in section 2200.

"(6) CYBER THREAT.—The term ‘cyber threat’ means—

"(A) has the meaning given the term ‘cybersecurity threat’ in section 2200; and

"(B) does not include any activity related to good faith security research, including participation in a bug-bounty program or a vulnerability disclosure program.

"(3) SEC. 2230. DEFINITIONS.

In this subtitle:

"(1) COVERED CYBER INCIDENT; COVERED ENTITY; CYBER INCIDENT.—The terms ‘covered cyber incident’, ‘covered entity’, and ‘cyber incident’ have the meanings given those terms in section 2230 of the Homeland Security Act of 2002, as added by section 5103 of this division.

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

"(5) INFORMATION SYSTEM; RANSOM PAYMENT; RANSOMWARE ATTACK; SECURITY VULNERABILITY.—The terms ‘information system’, ‘ransom payment’, ‘ransomware attack’, and ‘security vulnerability’ have the meanings given those terms in section 2200 of the Homeland Security Act of 2002, as added by section 5203 of this division.

"SEC. 5103. CYBER INCIDENT REPORTING.

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

(1) in section 2209(b) (6 U.S.C. 659(b)), as so redesignated by section 5203(b) of this division—

(A) in paragraph (11), by striking ‘and’ at the end;

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

(C) by adding at the end the following:

‘(13) receiving, aggregating, and analyzing reports related to covered cyber incidents (as defined in section 2230) submitted by covered entities (as defined in section 2230) and reports related to ransom payments submitted by entities in furtherance of the activities specified in sections 2202(e), 2203, and 2231, this subsection, and any other authorized activity of the Director, to enhance the situational awareness of cybersecurity threats across critical infrastructure sectors.’; and

(2) by adding at the end the following:

‘Subtitle C—Cyber Incident Reporting

‘SEC. 2230. DEFINITIONS.

In this subtitle:

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

‘(2) COUNCIL.—The term ‘Council’ means the Center established under section 2209.

‘(3) SEC. 2231. CYBER INCIDENT REVIEW.

The Center shall—

‘(a) ACTIVITIES.—The Center shall—

‘(1) receive, aggregate, analyze, and secure reports to lead the identification of tactics, techniques, and procedures used to perpetrate cyber incidents and ransomware attacks;

‘(2) leverage information gathered about cybersecurity incidents to—

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

‘(4) leverage information gathered about cybersecurity incidents to—

‘(5) for a covered cyber incident, as defined in subsection (a), that is below the micro-purchase threshold, does not include any activity related to good faith security research, including participation in a bug-bounty program or a vulnerability disclosure program.

‘(7) FEDERAL CONTRACTOR.—The term ‘Federal contractor’ means a business, nonprofit organization, or entity that holds a Federal Government contract or subcontract at any tier, grand, cooperative agreement, or other transaction agreement, unless that entity is a party only—

‘(A) a service contract to provide housekeeping or custodial services; or

‘(B) a contract to provide products or services unrelated to information technology that is below the micro-purchase threshold, as defined in section 2.101 of title 48, Code of Federal Regulations, or any successor regulation.

‘(8) FEDERAL ENTITY; INFORMATION SYSTEM; SECURITY CONTROL.—The terms ‘Federal entity’, ‘information system’, and ‘security control’ have the meanings given those terms in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

‘(9) SIGNIFICANT CYBER INCIDENT.—The term ‘significant cyber incident’ means a cybersecurity incident, or a group of related cybersecurity incidents, that the Secretary determines is likely to result in demonstrable harm to United States national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States.

‘(10) SMALL ORGANIZATION.—The term ‘small organization’—

‘(A) means—

‘(i) a small business concern, as defined in section 3 of the Small Business Act (15 U.S.C. 632); or

‘(ii) any nonprofit organization, including faith-based organizations and houses of worship, or other private sector entity with fewer than 200 employees (determined on a full-time equivalent basis); and

‘(B) does not include—

‘(i) a business, nonprofit organization, or other private sector entity that is a covered entity; or

‘(ii) a Federal contractor.

‘SEC. 2231. CYBER INCIDENT REVIEW.

The Center shall—

‘(a) ACTIVITIES.—The Center shall—

‘(1) receive, aggregate, analyze, and secure reports to lead the identification of tactics, techniques, and procedures used to perpetrate cyber incidents and ransomware attacks;

‘(2) leverage information gathered about cybersecurity incidents to—

‘(3) coordinate and share information with appropriate Federal departments and agencies to identify and track, and seize ransom payments, virtual currencies, to the greatest extent practicable;

‘(4) proactively identify opportunities and perform analyses, consistent with the protections in section 2235, to leverage and utilize data on cyber incidents in a manner that enables and strengthens cybersecurity research carried out by private sector organizations, to the greatest extent practicable; and

‘(5) for a covered cyber incident, including a ransomware attack, that also satisfies the definition of a significant cyber incident, or is part of a group of related cyber incidents that together satisfy such definition, coordinated in coordination with those covered cyber incident or group of those incidents and identity and disseminate ways to prevent or mitigate similar incidents in the future; in coordination with other divisions within the Agency, as appropriate;

‘(6) publish quarterly unclassified, public reports that may be released as the unclassified information contained in the briefings required under subsection (c);

‘(7) proactively identify opportunities and perform analyses, consistent with the protections in section 2235, to leverage and utilize data on ransomware attacks to support law enforcement investigations to identify, track, and seizing ransom payments, virtual currencies, to the greatest extent practicable;

‘(8) with respect to covered cyber incident reports under section 2232(a) and 2233 involving ongoing cyber threats or security vulnerabilities, immediately review those reports for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to appropriate stakeholders, in coordination with other divisions within the Agency, as appropriate;
tions 2232 and 2233, including—

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

"(12) on a not less frequently than annual basis, analyze public disclosures made pursuant to parts 229 and 223 of title 17, Code of Federal Regulations, or any subsequent document regulated by the Securities and Exchange Commission by entities experiencing cyber incidents and compare such disclosures to reports received by the Center; and

"(12) time after the covered cyber incident, ransom payment, or ransom payment information is submitted to the Director pursuant to section 2233, or information received pursuant to a request for information or subpoena under section 2234, make available the information to appropriate Sector Risk Management Agencies and other appropriate Federal agencies.

"(b) INTERAGENCY SHARING.— The National Cyber Director, in consultation with the Director and the Director of the Office of Management and Budget—

"(1) may establish a specific time requirement for sharing information under subsection (a)(13); and

"(2) shall determine the appropriate Federal agency to receive the report, under subsection (a)(13);

"(c) PERIODIC BRIEFING.—Not later than 60 days after the effective date of the final rule required under section 2232(b), and on the first day of each month thereafter, the Director, in consultation with the National Cyber Director, the Attorney General, and the Director of National Intelligence, shall provide to appropriate congressional committees, the minority leader of the Senate, the Speaker of the House of Representatives, the minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives, information, including the threat facing Federal agencies and covered entities, and applicable intelligence and law enforcement information, covered cyber incidents, and ransomware attacks, as of the date of the briefing,

"(1) including the total number of reports submitted under sections 2232 and 2233 during the preceding month, including a breakdown of required and voluntary reports;

"(2) identified trends in covered cyber incidents and ransomware attacks over the course of the preceding month and as contained in any reports, including any trends related to the information collected in the reports submitted under sections 2232 and 2233, including—

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

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

"(3) include a summary of the known uses of ransomware techniques, including any ransomware attacks against the covered entity that the Director not later than 72 hours after the covered cyber incident has occurred.

"(2) Ransom payment reports.—A covered entity that is a victim of a covered cyber incident shall report the covered cyber incident to the Director not later than 72 hours after the covered cyber incident reasonably believes that the covered cyber incident has occurred.

"(3) SUBSEQUENT RULEMAKINGS.—

"(a) GENERAL.—The Director is authorized to issue regulations to amend or revise the final rule issued pursuant to paragraph (1).

"(b) PROCEDURES.—Any subsequent rules issued under subparagraph (a) shall comply with the requirements under chapter 5 of title 5, United States Code, including the issuances of a notice of proposed rulemaking to implement subsection (a).
“(B) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetuate the covered cyber attack.

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

“(D) The name and other information that clearly identifies the entity that made the ransom payment.

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

“(F) The date of the ransom payment.

“(G) Details of any ransom payment instructions, including the type of virtual currency or other commodity requested, if applicable.

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

“(I) The amount of the ransom payment.

“(J) A clear description of the types of data required to be preserved pursuant to subsection (a)(4) and the period of time for which such data is required to be preserved.

“(K) Deadlines for submitting reports to the Director required under subsection (a)(3), which shall:

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

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

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

“(8) Procedures for—

“(A) entities to submit reports required by paragraphs (1), (2), and (3) of subsection (a), including the manner and form thereof, which shall include, at a minimum, a concise, user-friendly web-based form;

“(B) the Agency to carry out the enforcement provisions of section 2233, including with respect to the issuance, service, withdrawal, and enforcement of penalties, appeals and due process procedures, the suspension and debarment provisions in section 2234(c), and other aspects of noncompliance;

“(C) implementation of exceptions provided in subsection (a)(5); and

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

“(9) A clear description of the types of entities that covered cyber incident reports are required for purposes of section 2233(b)(7).

“(d) Third Party Report Submission and Ransom Payment .—

“(1) REPORT SUBMISSION.—An entity, including a covered entity, that is required to submit a covered cyber incident report or a ransom payment report shall submit a third-party report to the Director, such third party, such as an incident response company, insurance provider, service provider, information sharing and analysis organization, or law firm, so that the required report under subsection (a).

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

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

“(4) RESPONSIBILITY TO ADVISE.—Any third party used by an entity that knowingly makes a ransom payment on behalf of an entity impacted by a ransomware attack shall advise the impacted entity of responsibilities of the impacted entity regarding reporting ransom payments under this section.

“(e) Outreach to Covered Entities.—

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

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

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

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

“(C) An overview of the protections afforded to covered entities for complying with the requirements under paragraphs (1), (2), and (3) of section 2232(a).

“(D) An overview of the steps taken under section 2234 when a covered entity is not in compliance with the reporting requirements under subsection (a).

“(E) If the Director has reason to believe, whether through public reporting or other information in the possession of the Federal Government, including through analysis performed pursuant to paragraph (1) or (2) of section 2232(a), that an entity has experienced a covered cyber incident or ransom payment but failed to

“(F) An overview of the privacy and civil liberties protections under section 2235 applicable to ransom payments.

“(G)Any other entity as determined appropriate by the Director.

“(f) Organization of Reports.—Notwithstanding any ransom incident reports or ransom payments to the Director that are not required under paragraph (1), (2), or (3) of section 2232(a), but may enhance the situational awareness of cyber threats.

“(g) Voluntary Provision of Additional Information in Required Reports.—Entities may voluntarily include in reports required under paragraph (1), (2), or (3) of section 2232(a) information that is not required to be included, but that may enhance the situational awareness of cyber threats.

“(h) Application of Protections.—The protections under section 2235 applicable to covered cyber incident reports shall apply in the same extent to reports and information submitted under subsections (a) and (b).


“(a) Purpose.—In the event that an entity that is required to submit a report under section 2232(a) fails to comply with the requirements to report, the Director may obtain information about the incident or ransom payment by engaging the entity directly to request information about the incident or ransom payment, and, if the Director is unable to obtain information through such engagement, by issuing a subpoena to the entity, pursuant to subsection (c), to gather information sufficient to determine whether a covered cyber incident or ransom payment has occurred, and, if so, whether additional action is warranted pursuant to subsection (d).

“(b) Initial Request for Information.—

“(1) IN GENERAL.—If the Director has reason to believe, whether through public reporting or other information in the possession of the Federal Government, including through analysis performed pursuant to paragraph (1) or (2) of section 2232(a), that an entity has experienced a covered cyber incident or ransom payment, the Director may order the entity to submit timely reports or other information in the possession of the entity.
report such incident or payment to the Center within 72 hours in accordance with section 2232(a), the Director shall request additional information from the entity to confirm whether a covered cyber incident or ransom payment has occurred.

"(2) TREATMENT.—Information provided to the Center in response to a request under paragraph (1), or a subpoena issued pursuant to section 2232, shall be submitted through the reporting procedures established in section 2232.

"(c) AUTHORITY TO ISSUE SUBPOENAS AND DEBAR.—

"(1) IN GENERAL.—If, after the date that is 72 hours from the date on which the Director made a request for information pursuant to subsection (b), the Director has received no response from the entity from which such information was requested, or received an inadequate response, the Director may provide to such entity a subpoena to compel disclosure of information the Director deems necessary to determine whether a covered cyber incident or ransom payment has occurred and obtain the information required to be reported pursuant to section 2232 and any implementing regulations.

"(2) COURT ACTION.—

"(A) IN GENERAL.—If an entity fails to comply with a subpoena, the Director may file an action in the United States district court established in section 2232 for the Federal Government solely for—

"(i) a cybersecurity purpose;

"(ii) a cyber threat, including the source of a cybersecurity threat.

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

"(3) RULE OF CONSTRUCTION.—Nothing in this subtitle shall be construed to provide an enforcement mechanism to investigate or prosecute offenses listed in section 105(d)(5)(A)(v) of the Cybersecurity Act of 2015 (6 U.S.C. 2235(a), and subsection may not be delegated.

"(d) ACTIONS BY ATTORNEY GENERAL AND FEDERAL REGULATORY AGENCIES.—

"(1) IN GENERAL.—Notwithstanding section 2232(a) and subsection (b)(2) of this section, if the Attorney General or the appropriate Federal regulatory agency determines, based on information provided in response to a subpoena pursuant to subsection (c), that the facts relating to the covered cyber incident or ransom payment at issue may constitute grounds for a regulatory enforcement action or for criminal prosecution, the Attorney General or the appropriate Federal regulatory agency may use that information for a regulatory enforcement action or criminal prosecution.

"(2) APPLICATION TO CERTAIN ENTITIES AND THIRD PARTIES.—A covered cyber incident or ransom payment report submitted to the Center by an entity that makes a ransom payment or third party under section 2232 shall not be used by any Federal, State, local, Tribal, or territorial government or agency, contractor, or agent to undertake another law enforcement action against the entity that makes a ransom payment or third party.

"(g) AUTHORIZATION TO ISSUE SUBPOENAS AND DEBAR.—

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

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

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

"(h) PUBLICATION OF THE ANNUAL REPORT.

The Director shall publish a version of the annual report established in section 2232 on the website of the Agency, which shall include, at a minimum, the number of times the Director—

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

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

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

"SEC. 2235. INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT

"(a) DISCLOSURE, RETENTION, AND USE.—

"(1) AUTHORIZED ACTIVITIES.—Information provided required under subsection (b) to the Center in response to a request under section 2232 or 2235 may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

"(A) a cybersecurity purpose;

"(B) the purpose of identifying—

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

"(ii) a specific vulnerability;

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

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

"(E) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a cyber incident reported pursuant to section 2232 or 2235 or any of the offenses relating to cybersecurity contained in title 18 of this United States Code (the "Cybersecurity Act of 2015 (6 U.S.C. 1504(d)(5)(A)(v)).

"(2) AGENCY ACTIONS AFTER RECEIPT.—

"(A) RAPID, CONFIDENTIAL SHARING OF CYBER THREAT INDICATORS.—Upon receiving a covered cyber incident or ransom payment report regarding a cybersecurity threat indicator, the Director may exchange the information with a law enforcement agency or regulatory agency, or any State, local, Tribal, or territorial government to investigate or prosecute such offense.

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

"(C) PRIVACY AND CIVIL LIBERTIES.—Information contained in a covered cyber incident or ransom payment reports submitted to the Center in response to a request under section 2232 shall be retained, used, and disseminated, where permissible and appropriate, by the Federal Government in accordance with procedures to be developed for the protection of personal information consistent with processes adopted pursuant to section 105 of the Cybersecurity Act of 2015 (6 U.S.C. 1504), in a manner that protects from unauthorized use or disclosure any information that may contain—

"(A) personal information of a specific individual; or

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

"(D) DIGITAL SECURITY.—The Center and the Agency shall ensure that reports submitted to the Center or the Agency pursuant to section 2232, and any information contained in those reports, are collected, stored, and protected at a minimum in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standard Publication 199, or any successor documents.

"(E) PROHIBITION ON USE OF INFORMATION IN REGULATORY ACTIONS.—A State, local, or Tribal government shall not use information about a covered cyber incident or ransom payment obtained solely through reporting directly to the Center or the Agency in accordance with this subtitle to regulate, including through an enforcement action, the activities of the covered entity or entity that made a ransom payment.

"(F) NO WAIVER OF PRIVILEGE OR PROTECTION.—The submission of a report to the Center or the Agency under section 2232 shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection and attorney-client privilege.

"(G) EXEMPTION FROM DISCLOSURE.—Information contained in a report submitted to the Office under section 2232 shall be exempt from disclosure under section 552(b)(3)(B) of title 5, United States Code (commonly known as the Freedom of Information Act) and any State, Tribal, or local provision of law requiring disclosure of information or records.

"(H) EX PARTE COMMUNICATIONS.—The submission of a report to the Agency under section 2232 shall not be subject to a rule of any Federal agency or department or any judicial process pending in any court, to acquire from any person any communication with a decision-making official.

"(I) LIABILITY PROTECTIONS.—
"(1) IN GENERAL.—No cause of action shall lie or be maintained in any court by any person or entity and any such action shall be promptly dismissed for the submission of a report pursuant to subsection (a) that is solely based on the submission of a covered cyber incident report or ransom payment report to the Center or the Agency.

"(2) SCOPE.—The liability protections provided in subsection (e) shall only apply to or affect any action or proceeding by or on behalf of the United States, a State, or a political subdivision thereof, or any agency, instrumentality, or other entity or body, or any other authority of the United States, a State, or a political subdivision thereof, provided that nothing in this section shall create a defense to discovery or otherwise affect the discovery of any communication, document, material, or other record not created for the sole purpose of preparing, drafting, or submitting such report, may be received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, or any agency, instrumentality, or other entity or body, or any other authority of the United States, a State, or a political subdivision thereof, for any purpose.

"(g) PROPRIETARY INFORMATION.—Information contained in a report submitted to the Agency pursuant to this subtitle or any communication, document, material, or other record not created for the sole purpose of preparing, drafting, or submitting such report, may be received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, or any agency, instrumentality, or other entity or body, or any other authority of the United States, a State, or a political subdivision thereof, for any purpose.

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

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

"Subtitle C—Cyber Incident Reporting

"Sec. 2231. Cyber Incident Reporting.

"Sec. 2232. Required reporting of certain cyber incidents.

"Sec. 2233. Voluntary reporting of other cyber incidents.

"Sec. 2234. Notice required for ransom payment.

"Sec. 2235. Information shared with or provided to the Federal Government.

"SEC. 5104. FEDERAL SHARING OF INCIDENT REPORTS.

"(a) CYBER INCIDENT REPORTING SHARING.—

"(1) IN GENERAL.—Notwithstanding any other provision of law or regulation, any Federal agency, including any independent establishment (as defined in section 101 of title 5, United States Code), that receives a report from an entity of a cyber incident, including a ransomware attack, shall forward the report to the Director as soon as possible, but not later than 24 hours after receiving the report, unless a shorter period is required by an agreement made between the Cybersecurity Infrastructure Security Agency and the recipient Federal agency. The Director pursuant to this section shall forward the report pursuant to section 2231(b) of the Homeland Security Act of 2002, as added by section 5103 of this title.

"(2) RULE OF CONSTRUCTION.—The requirements described in paragraph (1) shall not be construed to be a violation of any provision of law or policy that would otherwise prohibit disclosure of such information.

"(3) PROTECTION OF INFORMATION.—The Director shall comply with any obligations of the recipient of such information as described in paragraph (1) to protect information, including with respect to privacy, confidentiality, or information security, if those obligations would otherwise preclude the communications or requirements made by this title or the amendments made by this title.

"(4) FOIA EXEMPTION.—Any report received by the Director pursuant to paragraph (1) shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code (commonly known as the ‘‘Freedom of Information Act’’).

"(b) CREATION OF COUNCIL.—Section 1752(c) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500) is amended—

"(1) in paragraph (1)—

"(A) in subparagraph (G), by striking ‘‘and’’ at the end; and

"(B) by redesignating subparagraph (H) as subparagraph (G);

"(2) in subparagraph (A)—

"(I) in subparagraph (i), by striking ‘‘the’’ and inserting ‘‘the Administration, the Depar tment of Homeland Security, and the”;

"(J) in subparagraph (ii), by striking ‘‘the’’ and inserting ‘‘the Administration, the Department of Homeland Security, and the”;

"(3) by adding at the end the following:

"‘‘(H) lead an intergovernmental Cyber Incident Reporting Council, in coordination with the Director of the Office of Management and Budget, the Attorney General, and the National Cyber Director and Infrastructure Security Agency and in consultation with sector Risk Management Agencies (as defined in section 2201 of the Homeland Security Act of 2002 (6 U.S.C. 651)) and other appropriate Federal agencies, to coordinate, deconflict, and harmonize Federal incident reporting requirements, including those issued through regulations, for covered entities (as defined in section 2230 of such Act) and entities that make a ransom payment (as defined in such section 2201 (6 U.S.C. 651); and)’’;

"(4) by adding at the end of paragraph (1) the following:

"‘‘(B) HARMONIZING REPORTING REQUIREMENTS.—The National Cyber Director shall, in consultation with the Director, the Attorney General, and the Director of the Office of Management and Budget, to the maximum extent practicable—

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

"(2) coordinate with the Director, the Attorney General, and regulatory authorities that receive reports relating to cyber incidents to identify duplicative, burdensome, or conflicting reporting processes, and where feasible, facilitate interagency agreements between such authorities to permit the sharing of such reports or other relevant information, including any applicable law, and to make recommendations for policy, without impacting the ability of such agencies to gain timely situational awareness of a covered cyber incident or ransom payment.

"SEC. 5105. RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM.

"(a) PROGRAM.—Not later than 1 year after the date of enactment of this Act, the Director shall establish a vulnerability warning program to leverage existing authorities and technology to specifically develop processes and procedures for, and to dedicate resources to managing information systems that contain security vulnerabilities associated with common ransomware attacks and to notify the owners of those vulnerable systems of their security vulnerability.

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

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

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

"(c) ENTITY NOTIFICATION.—If the Director is able to identify the entity at risk that owns or operates a vulnerable information system identified in subsection (b), the Director may notify such owner or operator.

"(2) NO IDENTIFICATION.—If the Director is not able to identify the entity at risk that owns or operates a vulnerable information system identified in subsection (b), the Director may utilize the subpoena authority pursuant to section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) to identify and notify the entity at risk pursuant to the procedures within that section.

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

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

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

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

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

"SEC. 5106. RANSOMWARE THREAT MITIGATION ACTIVITIES.

"(a) JUNIOR RANSOMWARE TASK FORCE.—

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

"(2) COMPOSITION.—The Joint Ransomware Task Force shall consist of participants from Federal agencies, as determined appropriate by the National Cyber Director, in consultation with the Secretary of Homeland Security.
(3) RESPONSIBILITIES.—The Joint Ransomware Task Force, utilizing only existing authorities of each participating agency, shall coordinate across the Federal Government activities to: 

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

(B) Consult with relevant private sector, State, local, Tribal, and territorial governments and international stakeholders to identify needs and establish mechanisms for priority Federal activities.

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

(D) Establishment of a framework and (i) prioritization for Federal action by appropriate Federal agencies; and (ii) identify metrics for success of said actions.


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

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

(G) Any other activities determined appropriate by the task force to mitigate the threat of ransomware attacks against Federal and non-Federal entities.

(H) Clarity of private sector law enforcement.

(i)Clarifying Private Sector Lawful Defensive Measures.—Not later than 180 days after the date of enactment of this Act, the National Cyber Director, in coordination with the Secretary of Homeland Security and the Attorney General, shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary of the Senate, the Committee on Homeland Security, the Committee on the Judiciary, and the Committee on Oversight and Reform of the House of Representatives a report that describes measures that private sector actors can take when countering ransomware attacks within each sector and what laws need to be clarified to enable that action.

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

SEC. 5107. CONGRESSIONAL REPORTING.

(a) REPORT ON STAKEHOLDER ENGAGEMENT.—Not later than 30 days after the date on which the Director issues the final rule under section 2232(b) of the Homeland Security Act of 2002, as added by section 5103(b) of this title, the Director shall submit to the Committees on Homeland Security in the Senate and the Committee on Homeland Security and Governmental Affairs in the Senate and the Committee on Homeland Security and Governmental Affairs in the House of Representatives a report that describes how the Director engaged stakeholders in the development of the final rule.

(b) REPORT ON OPPORTUNITIES TO STRENGTHEN SECURITY RESEARCH.—Not later than 1 year after the date of enactment of this Act, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and Governmental Affairs of the House of Representatives a report describing how the National Cybersecurity and Communications Integration Center established under section 415 of the Homeland Security Act of 2002 (6 U.S.C. 659) has carried out activities under section 2321(a)(9) of the Homeland Security Act of 2002, as added by section 5103(a) of this title, by proactively identifying opportunities to use cyber incident data to inform and enable cybersecurity research within the academic and private sector.

(c) REPORT ON RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM.—Not later than 1 year after the date of enactment of this Act, and annually thereafter for the duration of the pilot program established under section 5106, the Director shall submit to the Committees on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report, which may include a technical annex, describing the effectiveness of the pilot program, which shall include a discussion of the following:

(1) The effectiveness of the notifications under section 5105(c) in mitigating security vulnerabilities and the threat of ransomware.

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

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

(4) To the extent practicable, the number of vulnerable systems mitigated under this pilot by the Agency during the preceding year.

(d) REPORT ON HARMONIZATION OF REPORTING REGULATIONS.—

(1) IN GENERAL.—Not later than 180 days after the date on which the National Cyber Director convenes the Council described in section 2219(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)), the National Cyber Director shall submit to the appropriate congressional committees a report that includes—

(A) a list of duplicative Federal cyber incident reporting requirements on covered entities and entities that make a ransom payment;

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

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

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

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

(e) GAO REPORTS.—

(1) IMPLEMENTATION OF THIS TITLE.—Not later than 180 days after the date of enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Homeland Security and Governmental Affairs of the House of Representatives a report on the implementation of this title and the amendments made by this title.

(2) EXEMPTIONS TO REPORTING.—Not later than 1 year after the date on which the Director issues the final rule required under section 2232(b) of the Homeland Security Act of 2002, as added by section 5103 of this title, the Comptroller General of the United States shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the exemptions to reporting under paragraphs (1) and (5) of section 2232(a) of the Homeland Security Act of 2002, as added by section 5103 of this title, which shall include—

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

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

(C) an evaluation of the burden, financial and otherwise, on entities required to report cyber incidents under this title, including an analysis of entities that meet the definition of a small organization and would be exempt from reporting payments but not for being a covered entity; and

(D) a description of the consequences and effects of the exemptions.

(f) REPORT ON EFFECTIVENESS OF ENFORCEMENT MECHANISMS.—Not later than 1 year after the date on which the Director issues the final rule required under section 2232(b) of the Homeland Security Act of 2002, as added by section 5103 of this title, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the effectiveness of the enforcement mechanisms within section 2234 of the Homeland Security Act of 2002, as added by section 5103 of this title.

TITLE LI—CISA TECHNICAL CORRECTIONS AND IMPROVEMENTS ACT OF 2021

SEC. 5201. SHORT TITLE.

This title may be cited as the “CISA Technical Corrections and Improvements Act of 2021.”

SEC. 5202. REDesignations.

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

(1) by redesignating section 2217 (6 U.S.C. 665b) as section 2220;

(2) by redesignating section 2216 (6 U.S.C. 665c) as section 2219;

(3) by redesigning the fourth section 2215 (relating to Sector Risk Management Agencies) (6 U.S.C. 665c) as section 2217; and

(4) by redesigning the third section 2215 (relating to the Cybersecurity State Coordinator) (6 U.S.C. 665c) as section 2217, and

(b) Technical and Conforming Amendment—

(1) in section 2215 (relating to the Cybersecurity State Coordinator) (6 U.S.C. 665c) as section 2215, and

(2) Technical and Conforming Amendment—

(1) Amendment.—Section 904(b)(1) of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260) is amended—

(D) inserting the following:

SEC. 2200. DEFINITIONS.

Except as otherwise specifically provided, in this title—

(A) The term ‘Agency’ means the Cybersecurity and Infrastructure Security Agency.
"(2) AGENCY INFORMATION.—The term ‘agency information’ means information collected or maintained by or on behalf of an agency.

"(3) AGENCY INFORMATION SYSTEM.—The term ‘agency information system’ means an information system used or operated by an agency or by another entity on behalf of an agency.

"(4) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ‘appropriate congressional committees’ 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.

"(5) CLOUD SERVICE PROVIDER.—The term ‘cloud service provider’ means an entity offering products or services related to cloud computing as defined by the National Institutes of Standards and Technology in NIST Special Publication 800-145 and any amendment or superseding document relating thereto.

"(6) CRITICAL INFRASTRUCTURE INFORMATION.—The term ‘critical infrastructure information’ means information not customarily available to the public, as defined in § 8.4 of Standards and Technology in NIST Special Publication 800-145, and any amendment or superseding document relating thereto.

"(7) CYBER THREAT INDICATOR.—The term ‘cyber threat indicator’ means information that detects, predicts, or otherwise relates to an incident, including a description of the nature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting such information system.

"(8) CYBERSECURITY PURPOSE.—The term ‘cybersecurity purpose’ means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system to prevent, detect, or respond to an incident, including identifying and mitigating threats and vulnerabilities, and reducing impacts of cyber incidents.

"(9) CYBERSECURITY RISK.—The term ‘cybersecurity risk’ means a threat or vulnerability that may result in an unauthorized access to, unauthorized disclosure of, or unauthorized modification of, or deletion of an information system or information that is stored on, processed by, or transiting an information system.

"(10) CYBERSECURITY THREAT.—

"(A) In general.—Except as provided in subparagraph (B), the term ‘cybersecurity threat’ means an action, made or attempted by a person within the United States, on or through an information system that results in an unauthorized access to, unauthorized disclosure of, or unauthorized modification of, or deletion of an information system or information that is stored on, processed by, or transiting such information system.

"(B) Exclusion.—The term ‘cybersecurity threat’ does not include any action that solely involves a violation of a consumer term of service or a service use agreement.

"(11) DEFENSIVE MEASURE.—

"(A) In general.—Except as provided in subparagraph (B), the term ‘defensive measure’ means an action, device, procedure, signature, technique, or other measure applied to an information system or information stored on, processed by, or transiting such information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

"(B) Exclusion.—The term ‘defensive measure’ does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by—

(i) the entity operating the measure; or

(ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of the measure.

"(12) HOMELAND SECURITY ENTERPRISE.—The term ‘homeland security enterprise’ means the entity or Federal entity that is authorized to provide consent and has provided consent to another entity for operation of a defensive measure.

"(13) INCIDENT.—The term ‘incident’ means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system.

"(14) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term ‘information sharing and analysis organization’ means any formal or informal entity or collaboration thereof, operated by or on behalf of private sector organizations, for purposes of—

(A) gathering and analyzing critical infrastructure information, including information related to vulnerabilities and incidents, in order to better understand security problems and interdependencies related to critical infrastructure, including cybersecurity threats and vulnerabilities, and to protect critical information systems, so as to ensure the availability, integrity, and reliability thereof;

(B) communicating or disclosing critical infrastructure information, including cybersecurity risks and incidents, to help prevent, detect, mitigate, or recover from the effects of threats and vulnerabilities, such as ransomware attacks, to interrupt or disrupt the operation of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system.

"(15) INTELLIGENCE COMMUNITY.—The term ‘intelligence community’ has the meaning given in the section 3 of the National Security Act of 1947 (50 U.S.C. 3003(4)).

"(16) MANAGED SERVICE PROVIDER.—The term ‘managed service provider’ means an entity that delivers services, such as network, application, infrastructure, or security services, to Federal, State, local, and Federal Governments, or other entities operating critical infrastructure, for the purpose of improving the security and reliability thereof, to the extent it is related to such infrastructure information, including cybersecurity risks and incidents, to its members, State, local, and Federal Governments, or other entities operating critical infrastructure.

"(17) MONITOR.—The term ‘monitor’ means to acquire, identify, or scan, to possess, information that is stored on, processed by, or transiting an information system.

"(18) MONITOR.—The term ‘monitor’ means to acquire, identify, or scan, to possess, information that is stored on, processed by, or transiting an information system.

"(19) NATIONAL CYBERSECURITY ASSET RESPONSE ACTIVITIES.—The term ‘national cybersecurity asset response activities’ means—

(A) furnishing cybersecurity technical assistance to entities affected by cybersecurity threats or vulnerabilities; and

(C) assessing potential cybersecurity risks to a sector or region, including potential cascading effects, and developing courses of action to mitigate such risks;

(D) facilitating information sharing and operational coordination with threat responders;

(E) providing guidance on how best to utilize Federal resources and capabilities in a timely and effective manner to speed recovery from cybersecurity risks.

"(20) NATIONAL SECURITY SYSTEM.—The term ‘national security system’ has the meaning given in title 1103 of title 40, United States Code.

"(21) RANSOM PAYMENT.—The term ‘ransom payment’ means the transmission of any payment, virtual currency, or any portion thereof, which at any time been delivered as ransom in connection with a ransomware attack.

"(22) RANSOMWARE ATTACK.—The term ‘ransomware attack’ means—

(A) a cybersecurity incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operation of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system.

(B) does not include any such event where the demand for payment is made by a Federal entity, an international organization, or an entity funded by the National Science Foundation, or in response to an invitation by the owner or operator of the information system.
system for third parties to identify vulnerabilities in the information system.

(23) SECTOR RISK MANAGEMENT AGENCY.—The term ‘Sector Risk Management Agency’ means the Federal Emergency Management Agency, designated by law or Presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector in coordinating, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all hazards environment in coordinating with the Department.

(24) SECURITY CONTROL.—The term ‘security control’ means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

(25) SECURITY VULNERABILITY.—The term ‘security vulnerability’ means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

(26) SHARING.—The term ‘sharing’ (including all connotations thereof) means providing, receiving, and disseminating (including all connotations) of each such term.

(27) SUPPLY CHAIN COMPROMISE.—The term ‘supply chain compromise’ means a cyber incident within the supply chain of an information system that an adversary leverages to jeopardize the confidentiality, integrity, or availability of the information technology system or the system processes, stores, or transmits, and can occur at any point during the life cycle.

(28) VIRTUAL CURRENCY.—The term ‘virtual currency’ means the digital representation of a value, acting as a medium of exchange, a unit of account, or a store of value.

(29) VIRTUAL CURRENCY ADDRESS.—The term ‘virtual currency address’ means a system for third parties to identify vulnerabilities in the information system.

(i) in the matter preceding paragraph (1), by striking “subsection (c)” and inserting “subsection (b)”; and

(ii) in paragraph (1)(B)(ii), by striking “information sharing and analysis organizations” and inserting “Information Sharing and Analysis Organizations”;

(E) in subsection (j), as so redesignated, by striking reference to “(c)(7)” and inserting “(c)(8)”;

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

(i) in paragraph (1)(A), by striking “subsection (c)” and inserting “subsection (b)”; and

(ii) in paragraph (1)(B)(ii), by striking “(as defined in section 2220(b)(8))” and inserting “(as defined in section 2220(b)(7))”;

(G) in section 2210—

(A) by striking subsection (a); and

(B) by redesignating subsections (b) through (d) as subsections (a) through (c), respectively;

(H) in section 2211—

(i) in subsection (a), as so redesignated—

(I) in paragraph (1)—

(ii) in the matter preceding subparagraph (A), by striking “subsection (c)” and inserting “subsection (b)”;

(II) in subparagraph (B), by striking “subsection (c)” and inserting “subsection (b)”;

(iii) in subparagraph (C), by striking “subsection (c)” and inserting “subsection (b)”;

(iv) in subparagraph (D), by striking “subsection (c)” and inserting “subsection (b)”;

(v) in subparagraph (E), by striking “subsection (c)” and inserting “subsection (b)”;

(vi) in subparagraph (F), by striking “(as defined in section 2220(b)(7))” and inserting “subsection (b)”;

(vii) in subparagraph (G), by striking “subsection (c)” and inserting “subsection (b)”;

(viii) in subparagraph (H), by striking “subsection (c)” and inserting “subsection (b)”;

(ix) in subparagraph (I), by striking “subsection (c)” and inserting “subsection (b)”;

(x) in subparagraph (J), by striking “subsection (c)” and inserting “subsection (b)”;

(xi) in subparagraph (K), by striking “subsection (c)” and inserting “subsection (b)”;

(xii) in subparagraph (L), by striking “subsection (c)” and inserting “subsection (b)”;

(xiii) in subparagraph (M), by striking “subsection (c)” and inserting “subsection (b)”;

(xiv) in subparagraph (N), by striking “subsection (c)” and inserting “subsection (b)”;

(xv) in subparagraph (O), by striking “subsection (c)” and inserting “subsection (b)”;

(xvi) in subparagraph (P), by striking “subsection (c)” and inserting “subsection (b)”;

(xvii) in subparagraph (Q), by striking “subsection (c)” and inserting “subsection (b)”;

(xviii) in subparagraph (R), by striking “subsection (c)” and inserting “subsection (b)”;

(xix) in subparagraph (S), by striking “subsection (c)” and inserting “subsection (b)”;

(xx) in subparagraph (T), by striking “subsection (c)” and inserting “subsection (b)”;

(B) in subsection (o)(1)(A)(vi), by striking “section 2213(c)(5)”, and inserting “section 2213(b)(5)”; and
(4) in subsection (b)(6) (6 U.S.C. 1525(b)), by striking “section 2213(d)(2)”, and inserting “section 2213(c)(2)”.

(b) PUBLIC HEALTH SERVICE ACT.—Section 2811(b)(4)(D) of the Public Health Service Act (42 U.S.C. 248b(4)(D)) is amended by striking “section 228(c) of the Homeland Security Act of 2002 (6 U.S.C. 149(c))” and inserting “section 2209(b) of the Homeland Security Act of 2002”;


(1) in subsection (a)—

(2) in subsection (b), by striking “section 2201(5)” and inserting “section 2200”;

and
(3) in subsection (d)—
(A) by striking “section 2213” and inserting “section 2219”; and
(B) by striking “, as added by this section”;


(f) SMALL BUSINESS ACT.—Section 21(a)(b)(b) of the Small Business Act (15 U.S.C. 630a(a)(2)), as amended by striking “section 2209(a)” and inserting “section 2200”.


SA 4814. Ms. MURKOWSKI submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 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:

SEC. 1. EXTENSION OF AVAILABILITY OF CORONAVIRUS RELIEF FUND PAYMENTS TO TRIBAL GOVERNMENTS.

Section 601(d)(3) of the Social Security Act (42 U.S.C. 1302(d)(3)) is amended by inserting “, or, in the case of costs incurred by a Tribal government, during the period that begins on March 1, 2020, and ends on December 31, 2022)” before the period.

SA 4815. Mr. SANDERS submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 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 of subtitle G of title X, add the following:

SEC. 1064. REQUIREMENT OF DENTAL CLINIC OF DEPARTMENT OF VETERANS AFFAIRS IN EACH STATE.

The Secretary of Veterans Affairs shall ensure that each State has a dental clinic of the Department of Veterans Affairs to service the needs of the veterans within that State by not later than September 30, 2024.

SA 4816. Mr. COONS submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 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:

Subtitle — Sudan Democracy Act

SEC. 1. SHORT TITLE.
This subtitle may be cited as the “Sudan Democracy Act”.

SEC. 2. DEFINITIONS.
In this subsection—
(1) AMERICAN ALIEN.—The terms “admitted” and “alien” have the meanings given in section 101 of the Immigration and Nationality Act (8 U.S.C. 101).
(2) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term “appropriate congressional committees” means—
(A) the Committee on Foreign Relations of the Senate;
(B) the Committee on Appropriations of the Senate;
(C) the Committee on Foreign Affairs of the House of Representatives; and
(D) the Committee on Appropriations of the House of Representatives.
(3) FOREIGN PERSON.—The term “foreign person” means a person that is not a United States person.
(4) GROSS VIOLATIONS OF INTERNATIONALLY RECOGNIZED HUMAN RIGHTS.—The term “gross violations of internationally recognized human rights” has the meaning given such term in section 520B(d)(1) of the Foreign Assistance Act of 1961 (22 U.S.C. 2371(d)(1)).
(5) INTERNATIONAL FINANCIAL INSTITUTIONS.—The term “international financial institutions” means—
(A) the International Monetary Fund;
(B) the International Bank for Reconstruction and Development;
(C) the International Development Association;
(D) the International Finance Corporation;
(E) the Inter-American Development Bank; and
(F) the Asian Development Bank;

(G) the Inter-American Investment Corporation;

(H) the African Development Bank;

(I) the African Development Fund;

(J) the European Bank for Reconstruction and Development;

(K) the Multilateral Investment Guaranty Agency.

(6) KNOWN BY.—The term “knowingly” means, with respect to conduct, a circumstance, or a result, means that a person has actual knowledge, or should have known, that the conduct, the circumstance, or the result.

SEC. 3. FINDINGS; STATEMENT OF POLICY.

(a) FINDINGS.—Congress makes the following findings:

(1) On November 17, 1958, Lieutenant General Aboud al Hadi Ahmed alBagir of Sudan led the army’s first coup after independence, and the first successful coup in post-independence Africa.

(2) There have been more than 200 coup attempts across Africa since the 1958 coup in Sudan, including successful coups in Sudan in 1969, 1965, 1968, and 2019.

(3) On April 11, 2019, President Omar al Bashir of Sudan, who came to power in a military coup in 1989, was overthrown after months of popular protests by his own security chief, who established a Transitional Military Council, led by Lieutenant General Abdel Fattah al-Burhan, that ignored calls from the Sudanese people to transfer power to civilians.

(4) On August 17, 2019—

(A) the Transitional Military Council, under domestic and international pressure, signed a power-sharing agreement with the Forces for Freedom and Change, a broad coalition of political parties and civic groups representing the protest movement that had pushed for the end of the Bashir regime and a transition to civilian rule; and

(B) a transitional government was formed that allowed the junta leaders to remain in government in a partnership with new civilian authorities nominated by the Forces for Freedom and Change, including Prime Minister Abdullah Hamdok, for a transitional period to democracy.

(5) On October 25, 2021, Lieutenant General Burhan, with the support of Lieutenant Mohamed Hamdan Dagalo (also known as Hemedti’)—

(A) seized control of the Government of Sudan;

(B) deployed the military to the streets of Khartoum and Omdurman;

(C) shut down the internet in Sudan; and

(D) detained Prime Minister Hamdok and other civilian officials.

(6) The African Union Peace and Security Council has condemned the military takeover, rejected the unconstitutional change of
government, and on October 27, 2021, suspended Sudan from the Council until the civilian-led transitional government is restored.

The Sudanese people have condemned the military takeover and launched a campaign of civil disobedience, continuing the protests for democracy that began in late 2018 and reflecting a historic tradition of non-violence protest led by previous generations in Sudan against military regimes in 1964 and 1985.

In response to public calls for civilian rule since the February 2022 coup, Sudanese security forces have arbitrarily detained civilians and used excessive and lethal force against peaceful protesters that has resulted in civilian deaths across the country.

The October 25, 2021 military takeover represents a threat to—

(A) Sudan’s economic recovery and stability;

(B) the bilateral relationship between Sudan and the United States; and

(C) regional peace and security.

(b) SANCTIONS.—It is the policy of the United States—

(1) to support the democratic aspirations of the people of Sudan and a political transition process that results in a civilian government that is democratic, accountable, respects the human rights of its citizens, and is at peace with itself and with its neighbors;

(2) to encourage the reform of the security sector of Sudan to one that protects citizens under a democracy and respects civilian authority; and

(3) to deter military coups and efforts by external parties to support them.

SEC. 4. IMPOSITION OF SANCTIONS.

(a) IN GENERAL.—The President shall impose the sanctions described in subsection (b) with respect to any person or entity that the President determines, on or after the date of enactment of this Act—

(1) is responsible, complicit in, or directly or indirectly engaged or attempted to engage in—

(A) actions that undermine the transition to democracy in Sudan, or, after elections, undermine democratic processes or institutions;

(B) actions that threaten the peace, security, or stability of Sudan;

(C) actions that prohibit, limit, or penalize the exportation of expression or assembly by people in Sudan, or limit access to print, online, or broadcast media in Sudan;

(D) the arbitrary detention or torture of any person, or other gross violations of internationally recognized human rights in Sudan;

(E) significant efforts to impede investigations or other efforts to hold accountable serious human rights abuses in Sudan;

(F) actions that result in the misappropriation of significant state assets of Sudan or manipulation of the currency, or that hinder government oversight of parastatal budgets and revenues;

(G) actions that violate medical neutrality, including blocking access to care and targeting first responders, medical personnel, or medical institutions; or

(H) disrupting access to communication technologies and information on the internet;

(2) is an entity owned or controlled by any person or entity described in paragraph (1); or

(3) is acting for, or on behalf of, a person or entity referred to in paragraph (1), (2), or (3);

(4) is acting for, or on behalf of, a person or entity referred to in paragraph (1), (2), or (3);

(5) is an entity that is owned or controlled (directly or indirectly) by security and intelligence personnel, or foreign persons or entities described in paragraph (1) to receive significant revenue or financial benefit; or

(6) has knowingly—

(A) provided significant financial, material, or technological support—

(i) to a foreign person or entity described in paragraph (1) or an entity owned or controlled by such person or entity; or

(ii) received significant financial, material, or technological support from a foreign person or entity described in paragraph (1) or an entity owned or controlled by such person or entity;

(b) SANCTIONS; EXCEPTIONS.—

(1) SANCTIONS.—

(A) Asset blocking.—Notwithstanding section 202 of the International Emergency Economic Powers Act (50 U.S.C. 1701), the exercise of all powers granted to the President by such Act to order blocking of property and prohibit all transactions in all property and interests in property of a foreign person the President determines meets 1 or more of the standards in subsection (a) shall be subject to the penalties described in subsection (a) to the same extent as a person that commits an unauthorized act described in subsection (a) of such section.

(2) PENALTIES.—Any person that violates, conspires to violate, attempts to violate, or aids or abets the violation of any reporting, recordkeeping, or certification requirements under this section shall be subject to the penalties set forth in subsection (b) and (c) of section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705) to the same extent as a person that commits an unauthorized act described in subsection (a) of such section.

(c) WAIVER.—The President may annually waive the application of sanctions imposed on a foreign person pursuant to subsection (a) if the President—

(1) determines that such waiver with respect to such foreign person is in the national interest of the United States; and

(2) not later than the date on which such waiver will take effect, submits to the Congress a notification of, and justification for, such waiver to—

(A) the appropriate congressional committees;

(B) the Committee on Banking, Housing, and Urban Affairs of the Senate; and

(C) the Committee on Financial Services of the House of Representatives.

(d) SUNSET.—The requirement to impose sanctions under this section shall cease to be effective on December 31, 2026.

SA 4817. Ms. SINEMA submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4330, to authorize appropriations for fiscal year 2022 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.

SEC. 5. LAND TAKEN INTO TRUST FOR BENEFIT OF THE GILA RIVER INDIGENOUS COMMUNITY.

(a) DEFINITIONS.—In this section:

(1) BLACKWATER TRADING POST LAND.—The term “Blackwater Trading Post Land” means the approximately 56.3 acres of land as depicted on the map that—

(A) is located in Pinal County, Arizona, and bounded by Community land to the east, west, and north and State Highway 87 to the south; and

(B) is owned by the Community.

(2) COMMUNITY.—The term “Community” means the Gila River Indian Community of the Reservation.

(3) MAP.—The term “map” means the map entitled “Results of Survey, Ellis Property, A Portion of the West ½ of Section 12, Township 5 South, Range 7 East, Gila and Salt River Meridian, Pinal County, Arizona” and dated October 15, 2012.

(b) REQUIREMENT.—The term “Reservation” means the land located within the exterior boundaries of the reservation created under sections 3 and 4 of the Revised Statutes of 1851 (11 Stat. 401, chapter LXVI), and Executive orders of August 31, 1876, June 14, 1879,
May 5, 1982, November 15, 1883, July 31, 1911, June 2, 1913, August 27, 1914, and July 19, 1915, and any other lands placed in trust for the benefit of the Community.

(2) SECRETARY.—The term "Secretary" means the Secretary of the Interior.

(b) LAND TAKEN INTO TRUST FOR BENEFIT OF THE GILA RIVER INDIAN COMMUNITY.—

(1) IN GENERAL.—The Secretary shall take the Blackwater Trading Post Land into trust for the benefit of the Community, after the Community—

(A) submits to the Secretary a request to take the Blackwater Trading Post Land into trust for the benefit of the Community;

(B) conducts a survey (to the satisfaction of the Secretary) to determine the exact acreage and legal description of the Blackwater Trading Post Land, if the Secretary determines a survey is necessary; and

(C) pays all costs of any survey conducted under subparagraph (C).

(2) AVAILABILITY OF MAP.—Not later than 180 days after the Blackwater Trading Post Land is taken into trust under paragraph (1), the map shall be on file and available for public inspection in the appropriate offices of the Secretary.

(b) LAND TAKEN INTO TRUST PART OF RESERVATION.—After the date on which the Blackwater Trading Post Land is taken into trust under paragraph (1), the land shall be treated as part of the Reservation.

(c) GAMING.—Class II and class III gaming under the Indian Gaming Regulatory Act (25 U.S.C. 2701 et seq.) shall not be allowed at any time on the land taken into trust under paragraph (1).

(d) DESCRIPTION.—Not later than 180 days after the date of enactment of this Act, the Secretary shall submit the full metes and bounds description of the Blackwater Trading Post Land to be published in the Federal Register. The description shall, on publication, constitute the official description of the Blackwater Trading Post Land.

SA 4818. Mr. BENNET submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 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 of title XII, add the following:

Subtitle H—Long Wars Commission Act of 2021

SEC. 1291. SHORT TITLE. This subtitle may be cited as the "Long Wars Commission Act of 2021".

SEC. 1292. ESTABLISHMENT OF COMMISSION.

(a) ESTABLISHMENT.—There is established the Long Wars Commission (in this subtitle referred to as the "Commission").

(b) MEMBERSHIP.—

(I) IN GENERAL.—The Commission shall be composed of 12 members appointed as follows:

(A) One member appointed by the chair of the Committee on Armed Services of the Senate;

(B) One member appointed by the ranking minority member of the Committee on Armed Services of the Senate;

(C) One member appointed by the chair of the Committee on Foreign Relations of the Senate;

(D) One member appointed by the ranking minority member of the Committee on Foreign Relations of the Senate;

(E) One member appointed by the chair of the Committee on Armed Services of the House of Representatives;

(F) One member appointed by the ranking minority member of the Committee on Armed Services of the House of Representatives;

(G) One member appointed by the chair of the Committee on Foreign Affairs of the House of Representatives;

(H) One member appointed by the ranking minority member of the Committee on Foreign Affairs of the House of Representatives;

(I) One member appointed by the chair of the Senate Select Committee on Intelligence;

(J) One member appointed by the ranking minority member of the Senate Select Committee on Intelligence;

(K) One member appointed by the chair of the House Permanent Select Committee on Intelligence;

(L) One member appointed by the ranking minority member of the House Permanent Select Committee on Intelligence;

(2) DATE.—The appointments of the members of the Commission shall be made not later than 90 days after the date of enactment of this Act.

(3) PROHIBITIONS.—A member of the Commission appointed under subparagraph (A) may not—

(A) be a current member of Congress, or a former member of Congress, who served in Congress after January 3, 2001;

(B) have served in military or civilian positions having significant operational or strategic decisionmaking responsibilities for conducting United States Government activities in Afghanistan during the applicable period, or

(C) have been a party to any United States coalition defense contract during the applicable period.

(e) CO-CHAIRS.—The Commission shall constitute a quorum, and the Commission shall be filled in the same manner as the original appointment.

(f) MEETINGS.—

(1) INITIAL MEETING.—Not later than 30 days after the date on which all members of the Commission have been appointed, the Commission shall hold the first meeting of the Commission.

(2) FREQUENCY.—The Commission shall meet at the call of the co-chairs.

(3) QUORUM.—A majority of the members of the Commission shall constitute a quorum, but a lesser number of members may hold hearings.

(e) CO-CHAIRS.—

(1) DESIGNATION BY COMMITTEE CHAIRS.—The chair of the Committee on Armed Services of the Senate, the chair of the Committee on Foreign Relations of the Senate, the chair of the Committee on Armed Services of the House of Representatives, the chair of the Committee on Foreign Affairs of the House of Representatives, the chair of the Senate Select Committee on Intelligence, and the chair of the House Permanent Select Committee on Intelligence shall jointly designate one member of the Commission to serve as co-chair of the Commission.

(2) DESIGNATION BY RANKING MINORITY MEMBERS.—The ranking minority member of the Committee on Armed Services of the Senate, the ranking minority member of the Committee on Foreign Affairs of the Senate, the ranking minority member of the Committee on Armed Services of the House of Representatives, and the ranking minority member of the Committee on Foreign Affairs of the House of Representatives, the ranking minority member of the Senate Select Committee on Intelligence, and the ranking minority member of the House Permanent Select Committee on Intelligence shall jointly designate one member of the Commission to serve as co-chair of the Commission.

SEC. 1293. DUTIES.

(a) REVIEW.—The Commission shall review United States involvement in the conflicts in Afghanistan and Iraq beginning during the period prior to the September 11, 2001, attacks and ending on September 1, 2022, including military engagement, diplomatic efforts, economic assistance, reconstruction efforts, foreign assistance, congressional oversight, and withdrawal in such conflicts.

(b) ASSESSMENT AND RECOMMENDATIONS.—

(1) conduct a comprehensive assessment of United States involvement in the conflicts in Afghanistan and Iraq, including:

(A) United States military, diplomatic, and political objectives in the conflicts, and the extent to which those objectives were achievable;

(B) an evaluation of the interagency decisionmaking processes during the campaigns;

(C) an evaluation of the United States military’s conduct during the campaigns and the extent to which its operational approach compromised campaign progress;

(D) any regional and geopolitical threats to the United States resulting from the conflicts;

(E) the extent to which initial United States national objectives for the conflicts were met;

(F) the long-term impact on United States relations with allied nations who participated in the Iraq and Afghanistan conflicts;

(G) the effectiveness of counterterrorism, counterinsurgency, and security force assistance strategies employed by the United States military;

(H) the effect of United States involvement in the conflicts on the readiness of the United States Armed Forces;

(I) the effect of United States involvement in the conflicts on civil-military relations in the United States;

(J) the implications of the use of funds for overseas contingency operations as a mechanism for funding United States involvement in the conflicts;

(K) any other matters in connection with United States involvement in the conflicts that the Commission considers appropriate;

(2) identify circumstances under which conflict presents a significant likelihood of developing into an irregular or civil war; and

(3) develop recommendations based on the assessment, as well as any other information the Commission considers appropriate, for relevant questions to be asked during future deliberations by Congress of authorization for use of military force in conflicts that have the potential to develop into an irregular or civil war.

(c) REPORT.—

(1) FINAL REPORT.—Not later than 2 years after the date of the enactment of this Act, the Commission shall submit to the President, the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, the Committee on Armed Services of the House of Representatives, the Committee on Armed Services of the Senate, the Committee on Foreign Relations of the Senate, the Committee on Foreign Affairs of the House of Representatives, the Senate Select Committee on Intelligence, and the House Permanent Select Committee on Intelligence a report on the Commission’s findings, conclusions, and recommendations of the Commission under this section. The report shall do each of the following:
(A) Provide an assessment of the current security, political, humanitarian, and economic situation in Afghanistan and Iraq.

(B) Provide lessons learned from United States involvement in and withdrawal from, the conflicts in Afghanistan and Iraq.

(C) Provide recommendations on questions to be asked during future deliberations by Congress of an authorization for use of military force in a conflict that has the potential to develop into an irregular war.

(D) Address any other matters with respect to United States involvement in the conflicts in Afghanistan and Iraq that the Commission considers appropriate.

(E) Provide recommendations about United States policies and strategic choices that influence the use of military force and nation-building, in future foreign policy engagements.

(F) Provide recommendations about the need to foster any new alliances necessary to future foreign policy engagements.

(2) INTERIM BRIEFING.—Not later than one year after the date of the enactment of this Act, the Commission shall provide to the committees of Congress and the officials referred to in paragraph (1) a briefing on the status of its review and assessment under subsection (1), together with a discussion of any interim recommendations developed by the Commission as of the date of the briefing.

(3) FORM OF REPORT.—The report submitted to Congress under paragraph (1) shall be submitted in unclassified form. The report shall also include a classified annex.

SEC. 1294. POWERS OF COMMISSION.

(a) HEARINGS.—The Commission may hold such hearings, sit and act at such times and places, take such testimony, and receive such evidence as the Commission considers advisable to carry out this subtitle.

(b) ASSISTANCE FROM FEDERAL AGENCIES.—

(1) INFORMATION.—

(A) IN GENERAL.—The Commission may secure directly from a Federal department or agency such information as the Commission considers necessary to carry out this subtitle.

(B) REQUESTS TO OTHER FEDERAL AGENCIES.—The Commission may request the head of a Federal department or agency to provide the Commission with the information referred to in paragraph (A). The head of the department or agency shall provide the requested information to the Commission without reimbursement.

(c) FURNSHING INFORMATION.—On request of the co-chairs of the Commission, the head of the department or agency shall expeditiously furnish the information to the Commission.

(d) GENERAL SERVICES.—Upon the request of the Commission, the Administrator of General Services shall provide to the Commission, on a reimbursable basis, the administrative assistance and office space necessary for the Commission to carry out its purposes and functions under this subtitle.

(e) POSTAL SERVICES.—The Commission may use the United States mails in the same manner and under the same conditions as other departments and agencies of the Federal Government.

(f) GIFTS.—The Commission may accept, use, and dispose of gifts or donations of services or property.

(g) COOPERATION FROM UNITED STATES GOVERNMENT.—

(1) IN GENERAL.—The Commission shall receive the full and timely cooperation of the Secretary of Defense, the Secretary of State, and the Director of National Intelligence in providing the Commission with analyses, briefings, and other information necessary for the discharge of the duties of the Commission.

(2) LIAISON.—The Secretary of Defense, the Secretary of State, and the Director of National Intelligence shall each designate at least one officer or employee of their respective organizations to serve as a liaison officer to the Commission.

SEC. 1295. COMMISSION PERSONNEL MATTERS.

(a) COMPENSATION OF MEMBERS.—A member of the Commission who is not an officer or employee of the Federal Government shall be paid at the rate of $200 per day (including travel time) during which the member is engaged in the performance of the duties of the Commission.

(b) TRAVEL EXPENSES.—A member of the Commission shall be allowed travel expenses, including per diem in lieu of subsistence, at rates authorized for agencies under subchapter I of chapter 57 of title 5, United States Code, while away from their homes or regular places of business in the performance of services for the Commission.

(c) STAFF.—

(1) IN GENERAL.—The co-chairs of the Commission may, without regard to the civil service laws (including regulations), appoint and terminate an executive director and such other personnel as the co-chairs consider necessary to carry out the duties of the executive director and other personnel.

(2) COMPENSATION.—The co-chairs may fix the compensation of the executive director and other personnel.

(3) PERSONNEL MATTERS.—The authority to fix personnel matters under paragraph (1) is subject to the confirmation by the Commission.

(4) PRACTICES.—The co-chairs may establish practices for the performance of services for the Commission.

(5) APPOINTMENTS.—The co-chairs may appoint, without regard to the civil service laws (including regulations), except that the employment of an executive director shall be subject to confirmation by the Commission.

(b) THE COMMISSION.—The co-chairs may appoint contractors and consultants as the Commission considers necessary to carry out the duties of the Commission.

(c) PERSONNEL MATTERS.—The authority to fix personnel matters under paragraph (1) is subject to the confirmation by the Commission.

(3) FORM.—The report required by subsection (a) shall include a detailed summary of each of the following for each combatant command:

(1) Activities undertaken as of the date on which the report is submitted to combat the threats posed by illegal, unreported, and unregulated fishing.

(2) Coordination among the United States Armed Forces, partner countries, and public-private partnerships to combat the threats described in paragraph (1).

(3) Efforts undertaken to support unclassified data integration, analysis, and delivery with regional partners to combat the threats described in paragraph (1).

(4) Information sharing and coordination with efforts of the Interagency Working Group on IUU Fishing.

(b) ELEMENTS.—The report required by subsection (a) shall include a description of the following:

(1) Activities undertaken as of the date on which the report is submitted to combat the threats posed by illegal, unreported, and unregulated fishing.

(2) Coordination among the United States Armed Forces, partner countries, and public-private partnerships to combat the threats described in paragraph (1).

(3) Efforts undertaken to support unclassified data integration, analysis, and delivery with regional partners to combat the threats described in paragraph (1).

(4) Information sharing and coordination with efforts of the Interagency Working Group on IUU Fishing.

(5) Best practices and lessons learned from ongoing and previous efforts relating to the threats described in paragraph (1), including strategies for coordination and successes in public-private partnerships.

(6) Limitations related to affordability, resource constraints, or other factors that constrain the success or expansion of efforts related to the threats described in paragraph (1).

(7) Any new authorities needed to support efforts to combat the threats described in paragraph (1).

(c) FORM.—The report required by subsection (a) shall be submitted in unclassified form, but may include a classified annex.

(d) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term “appropriate committees of Congress” means—

(A) Committee on Armed Services, the Committee on Commerce, Science, and Transportation, the Committee on Foreign Relations, and the Committee on Appropriations of the Senate; and

(B) the Committee on Armed Services, the Committee on Commerce, Science, and Transportation, and the Committee on Appropriations of the House of Representatives.

(2) INTERAGENCY WORKING GROUP ON IUU FISHING.—The term “Interagency Working Group on IUU Fishing” means the working group established by section 3552 of the Magnuson-Stevens Fishery Conservation and Management Act (16 U.S.C. 1802).

SEC. 1297. AUTHORIZATION OF APPROPRIATIONS.

(a) IN GENERAL.—There is authorized to be appropriated to the Commission such amounts as necessary to carry out activities under this subtitle.

(b) AVAILABILITY.—Any sums appropriated under this section shall remain available, without fiscal year limitation, until expended.
SA 4820. Mr. COTTON (for himself, Mr. MANCHIN, Mr. TUBERVILLE, and Mr. KELLY) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 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:

**Title II—Extraction and Processing of Critical Minerals in the United States**

**SEC. 1431. SHORT TITLE.**

This title may be cited as the “Restoring Essential Energy and Security Holdings Onshore for Rare Earths and Critical Minerals Act of 2021” or the “REShore Critical Minerals Act of 2021.”

**SEC. 1432. DEFINITIONS.**

In this subtitle:

(A) the term “appropriate congressional committees” means—

(1) the Committee on Armed Services, the Committee on Foreign Relations, the Committee on Natural Resources, the Committee on Commerce, Science, and Transportation, and the Select Committee on Intelligence of the Senate; and

(B) the Committee on Armed Services, the Committee on Foreign Affairs, the Committee on Energy and Commerce, and the Permanent Select Committee on Intelligence of the House of Representatives.

(B) the term “critical mineral” has the meaning given that term in section 7062(a) of the Energy Act of 2020 (division Z of Public Law 116–266; 30 U.S.C. 1606(a)).

(3) the term “defense mineral product” means any product—

(A) formed or comprised of, or manufactured from, one or more critical minerals; and

(B) used in critical military defense technologies or other related applications of the Department of Defense.

(4) the term “processed or refined” means any process by which a defense mineral is extracted, separated, or otherwise manipulated to render the mineral usable for manufacturing a defense mineral product.

**SEC. 1433. REPORT ON STRATEGIC CRITICAL MINERAL AND DEFENSE MINERAL PROJECTS RESERVE.**

(a) FINDINGS.—Congress finds that the storage of substantial quantities of critical minerals and defense mineral products will—

(1) improve the reliability of the United States to the effects of a severe supply chain interruption; and

(2) provide limited protection from the short-term consequences of an interruption in supplies of defense mineral products.

(b) SENSE OF CONGRESS.—It is the sense of Congress that securing critical minerals and defense mineral products that the Secretary of Defense should prioritize procurement of critical minerals and defense mineral products that are assured to the United States, including that are mined, produced, separated, and manufactured within the United States.

(c) REPORT REQUIRED.—

(1) the department shall submit, not later than 70 days after the date of the enactment of this Act, the Secretary of the Interior, acting through the United States Geologic Survey, and the Secretary of Defense, in consultation with the Secretary of Homeland Security, the Director of the Cybersecurity and Infrastructure Security Agency, and the Director of National Intelligence, shall jointly submit to the appropriate congressional committees a report—

(A) describing the existing authorities and funding levels of the Federal Government to stockpile critical minerals and defense mineral products;

(B) assessing whether these authorities and funding levels are sufficient to meet the requirements of the United States; and

(C) including recommendations to diminish the vulnerability of the United States to disruptions in the supply chains for critical minerals and defense mineral products through changes to policy, procurement regulations, or existing law, including any additional statutory authorities that may be needed.

(2) CONSIDERATIONS.—In developing the report required by paragraph (1), the Secretary of the Interior, the Secretary of Defense, the Secretary of Commerce, the Secretary of Homeland Security, the Director of the Cybersecurity and Infrastructure Security Agency, and the Director of National Intelligence shall take into consideration the needs of the Armed Forces of the United States, communications (as defined in section 3(c) of the National Security Act of 1947 (50 U.S.C. 3009(c))), the defense industrial and technology sectors, and any physical infrastructure, cybersecurity and digital infrastructure designated as critical to the national security of the United States.

**SEC. 1434. REPORT ON DISCLOSURES CONCERNING CRITICAL MINERALS BY CONTRACTORS OF DEPARTMENT OF DEFENSE.**

(a) REPORT REQUIRED.—Not later than December 31, 2022, the Secretary of Defense, after consultation with the Secretary of Commerce, the Secretary of State, and the Secretary of the Interior, shall submit to the appropriate congressional committees a report that includes—

(1) a review of the existing disclosure requirements with respect to the provenance of magnets used within defense mineral products; and

(2) a review of the feasibility of imposing a requirement that any contractor of the Department of Defense provide a disclosure with respect to any system with a defense mineral product that is a permanent magnet, including an identification of the country or countries in which—

(A) the critical minerals used in the magnet were mined;

(B) the critical minerals were refined into oxides;

(C) the critical minerals were made into metals and alloys; and

(D) the magnet was sintered or bonded and magnetized; and

(3) recommendations to Congress for implementing such a requirement, including methods to ensure that any tracking or provenance system is independently verifiable.

**SEC. 1435. REPORT ON PROHIBITION ON ACQUISITION OF DEFENSE MATERIALS FROM NON-ALLIED FOREIGN NATIONS.**

The Secretary of Defense shall study and submit to the appropriate congressional committees a report on the potential impacts of imposing a restriction that, for any contract entered into or renewed on or after December 31, 2026, for the procurement of a system the export of which is restricted or controlled under the Arms Export Control Act (22 U.S.C. 2751 et seq.), no critical minerals processed or refined in the People’s Republic of China may be included in the system.

**SEC. 1436. PRODUCTION IN AND USES OF CRITICAL MINERALS BY UNITED STATES ALLIES.**

(a) POLICY.—It shall be the policy of the United States to encourage countries that are allies of the United States to identify alternatives, to the maximum extent practicable, to the use of critical minerals from foreign entities of concern or countries that such Secretaries deem to be of concern; and

(b) REPORT REQUIRED.—Not later than December 31, 2022, and annually thereafter, the Secretary of Defense, in coordination with the Secretary of State, shall submit to the appropriate congressional committees a report—

(1) describing the discussions of such Secretaries with countries that are allies of the United States concerning supply chain security for critical minerals; and

(2) assessing the likelihood of those countries identifying alternatives, to the maximum extent practicable, to the use of critical minerals from foreign entities of concern or countries that such Secretaries deem to be of concern; and

(3) assessing initiatives in other countries to increase critical mineral mining and production capabilities.

**SEC. 1437. PRIMARY INSTITUTE FOR DEFENSE RESEARCH.**

(a) PLAN TO PROMOTE DEFENSE RESEARCH AT MINORITY INSTITUTIONS.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Secretary of Defense shall submit to the congressional defense committees a plan (in this section referred to as the “Plan”)—

(A) to promote defense research activities at minority institutions to elevate the defense research capacity of minority institutions; and

(B) for the establishment of the Minority Institute for Defense Research (in this section referred to as the “Institute”).

(b) ELEMENTS.—The Plan shall include the following:

(1) An assessment relating to the engineering, research, and development capabilities, including the workforce, administrative support, and physical infrastructure, of minority institutions and their ability to participate in defense research and engineering activities and effectively compete for defense research contracts;

(2) An assessment of the activities and investments necessary to elevate minority institutions or a consortium of minority institutions to parity with research institutions and universities, to the level of R1 research institutions and increase their participation...
in, and ability to effectively compete for, defense research and engineering activities.

(C) Recommendations relating to actions that may be taken by the Department of Defense, minority-serving institutions to establish the Consortium within 3 years.

(D) The specific goals, incentives, and metrics developed by the Secretary in subsection (a) and amended effective competition for Federal research and development needs of the Department.

(3) DETERMINATION.—In developing the plan under paragraph (1), the Secretary shall consult with such other public and private sector organizations as the Secretary considers appropriate.

(4) PUBLICLY AVAILABLE.—The Secretary shall post the Plan on a publicly available website of the Department.

(5) MINORITY INSTITUTION DEFINED.—In this subsection, the term ‘minority institution’ means—

(A) a part B institution (as such term is defined in section 322 of the Higher Education Act of 1965 (20 U.S.C. 1061)); or

(B) an accredited minority institution (as such term is defined in section 365 of the Higher Education Act of 1965 (20 U.S.C. 1061k)).

(b) ACTIVITIES TO SUPPORT RESEARCH AND ENGINEERING ORGANIZATIONS TO COLLABORATE WITH HISTORICALLY BLACK COLLEGES AND UNIVERSITIES AND MINORITY-SERVING INSTITUTIONS OF HIGHER EDUCATION.—Subsection (c) of section 2362 of title 10, United States Code, is amended—

(1) by redesignating paragraph (4) as paragraph (5); and

(2) by inserting after paragraph (3) the following new paragraph:

‘‘(4) Developing the capability, including workforce, administrative support, and research infrastructure (including physical), of covered educational institutions to more effectively compete for Federal research and engineering funding opportunities.’’.

(c) INCREASING INCENTIVES FOR NATIONAL SECURITY RESEARCH AND ENGINEERING ORGANIZATIONS TO COLLABORATE WITH HISTORICALLY BLACK COLLEGES AND UNIVERSITIES AND MINORITY-SERVING INSTITUTIONS OF HIGHER EDUCATION.—Subsection (d) of such section is amended—

(1) by striking ‘‘The Secretary of Defense may define’’ and inserting ‘‘The Secretary of Defense shall’’—

‘‘(1) develop’’;

(2) in paragraph (1), as designated by paragraph (1) of such subsection, the period at the end and inserting ‘‘; and’’; and

(3) by adding at the end the following new paragraph:

‘‘(2) establish goals and incentives for each federally funded research and development center, science and technology reinvestment laboratory, and university-affiliated research center to increase and measure the capacity of covered educational institutions to address the research and development needs of the Department through partnerships and collaborations.’’.

(d) INCREASING PARTNERSHIPS FOR MINORITY INSTITUTIONS WITH NATIONAL SECURITY RESEARCH AND ENGINEERING ORGANIZATIONS.—Such section is amended—

(1) by redesigning subsections (e) and (f) as (f) and (g) respectively; and

(2) by inserting after subsection (d) the following new subsection:

‘‘(e) PARTNERSHIPS.—The Secretary of Defense shall—

(1) require the core capabilities of each university-affiliated research center to include partnerships with covered educational institutions as part of the educational research center’s mission;

(2) require in each indefinite delivery, indefinite quantity established or renewed with a university-affiliated research center to establish or maintain a partnership with a specific covered educational institution or consortium of covered educational institutions to provide the Department with capacity building at such covered educational institution or covered educational institutions;

(3) require each university-affiliated research center to report annually on their subcontracts and other activities with covered educational institutions; and

(4) post on a publicly available website of the Department a list of covered educational institutions and their defense research capabilities.’’.

(e) DEFINITION OF UNIVERSITY-AFFILIATED RESEARCH CENTERS.—Subsection (g) of such section, as redesignated by subsection (d)(1), is amended to read as follows:

‘‘(1) ‘DEFINITION OF UNIVERSITY-AFFILIATED RESEARCH CENTER.’’—

‘‘(1) the term ‘covered educational institution’ means—

(A) an institution of higher education eligible to receive, under title III or V of the Higher Education Act of 1965 (20 U.S.C. 1051 et seq.); or

(B) an accredited postsecondary minority institution;

(2) ‘The term ‘university-affiliated research center’ means a research organization within an institution of higher education (as defined in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001)) that—

‘‘(A) provides or maintains Department essential engineering, research, or development capability; and

‘‘(B) receives sole source contract funding from the Department pursuant to section 230(c)(3) of this title.’’.

SEC. 853. FUNDING FOR APPLIED AND ADVANCED TECHNOLOGY DEVELOPMENT AT HISTORICALLY BLACK COLLEGES AND UNIVERSITIES AND MINORITY INSTITUTIONS.

(a) ADDITIONAL FUNDING.—

(1) APPLIED RESEARCH.—(A) The amount authorized to be appropriated for fiscal year 2022 by section 201 for research, development, test, and evaluation is hereby increased by $10,000,000, with an amount of the increase to be available for Advanced Research and Development.

(B) The amount available under subparagraph (A) shall be available for minority institutions.

(2) ADVANCED TECHNOLOGY DEVELOPMENT.—(A) The amount authorized to be appropriated for fiscal year 2022 by section 201 for research, development, test, and evaluation is hereby increased by $10,000,000, with the amount of the increase to be available for Advanced Technology Development.

(B) The amount available under subparagraph (A) shall be available for minority institutions.

(b) DETERMINATION.—The amount authorized to be appropriated for fiscal year 2022 by section 201 for research, development, test, and evaluation is hereby increased by $10,000,000, with the amount of the increase to be available for Advanced Technology Development.

(c) SAVINGS CLAUSE.—No determination made under section (a) shall impact the current filing and reimbursement process for the Secure and Trusted Communications Networks Reimbursement Program at the Federal Communications Commission.

(d) DEFINITIONS.—In this section—

(1) the term ‘access’ means optical fiber and optical fiber cable that connects buildings or similar organizational governance bodies and the day-to-day management and administration of business operations as overseen by principals.

(2) the term ‘control’ means the ability to determine the outcome of decision-making by a company through the strategic policy setting exercised by boards of directors or similar organizational governance bodies and the day-to-day management and administration of business operations as overseen by principals.

(3) the term ‘long haul’ means optical fiber and optical fiber cable that connects cities and metropolitan areas.

(4) the term ‘metro’ means optical fiber and optical fiber cable that connects city
business districts and central city and suburban areas.

The term “passive” means unpowered optical fiber and optical fiber cable.

SA 4823. Mr. MARKEY submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 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:

Strike section 6505 and insert the following:

SEC. 6505. BRIEFING ON CONSULTATIONS WITH UNITED STATES ALLIES REGARDING NUCLEAR POSTURE REVIEW.

(a) In general.—Not later than January 31, 2022, the Secretary of Defense, in coordination with the Secretary of State, shall brief the appropriate congressional committees on all consultations with United States allies and related matters regarding the 2021 Nuclear Posture Review.

(b) Elements.—The briefing required by subsection (a) shall include the following:

(1) A listing of all countries consulted with respect to the Nuclear Posture Review, including the dates and circumstances of each such consultation and the countries present.

(2) An overview of the topics and concepts discussed with each such country during such consultations, including any discussion of potential changes to the nuclear declaratory policy of the United States.

(3) A summary of any feedback provided during such consultations.

(4) A description of the consultations conducted by the Department of Defense and the Department of State with experts outside such departments and civil society organizations with respect to the 2021 Nuclear Posture Review.

(5) A listing of the consultants who participated in the 2021 Nuclear Posture Review in a formal capacity.

(6) An identification of the options related to United States nuclear force structure and nuclear doctrine that were presented to the President by the Department of Defense.

SA 4824. Mr. BARRASSO submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 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 of subtitle G of title X, add the following:

SEC. 1064. ENSURING CONSIDERATION OF THE NATIONAL SECURITY IMPACTS OF URANIUM AS A CRITICAL MINERAL.

(a) In general.—The Secretary of Defense, in coordination with the Secretary of Energy, the Secretary of the Interior (acting through the Director of the United States Geological Survey), and the Secretary of Commerce, shall conduct an assessment of the effect on national security that may result from uranium ceasing to be designated as a critical mineral by the Secretary of the Interior pursuant to section 7002(c) of the Energy Act of 2020 (division Z of Public Law 116–260; 30 U.S.C. 1606(c)).

(b) Report.—Not later than 180 days after enactment of this Act, the Secretary of Defense shall submit to the appropriate committees of Congress a report on the findings of the assessment conducted under subsection (a), including an assessment of—

(1) any effects the change in designation described in that subsection may have on domestic uranium production;

(2) any effects of the reliance of the United States on imports of uranium from foreign sources, including United States–owned entities, to supply fuel for commercial reactors;

(3) the effects of such reliance and other factors on the domestic production, conversion, fabrication, and enrichment of uranium as it relates to national security, including energy security purposes; and

(4) any effects on Federal national security programs, including existing and future uses of unobligated, United States–origin uranium.

(c) RECOMMENDATION ON URANIUM CRITICAL MINERAL DESIGNATION.—The report required by subsection (b) shall include a recommendation to the Secretary of the Interior regarding whether it is in the interest of the United States to consider uranium for future designation as a critical mineral pursuant to section 7002(c) of the Energy Act of 2020 (division Z of Public Law 116–260; 30 U.S.C. 1606(c)).

(d) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this section, the term ‘appropriative committee of Congress’ means—

(1) the Committee on Armed Services, the Committee on Energy and Natural Resources, the Committee on Commerce, Science, and Transportation of the Senate; and

(2) the Committee on Armed Services, the Committee on Energy and Commerce, and the Committee on Natural Resources of the House of Representatives.

SA 4825. Mr. BARRASSO submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 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:

SEC. HA-LEU FOR ADVANCED NUCLEAR REACTOR DEMONSTRATION PROJECTS.—

(1) ACTIVITIES.—Not later than 30 days after the date of enactment of the National Defense Authorization Act for Fiscal Year 2023, the Secretary shall initiate activities to make available HA-LEU, produced from inventories owned by the Department, for use by advanced nuclear reactors, with priority given to the awarding to the Department of Energy, in consultation with the Secretary of Defense, of funding opportunity announcement of the Department numbered DE-FA00-002271 for Pathway 1, Advanced Reactor Demonstrations, with additional, where applicable, HA-LEU to be made available to members of the consortium established under subsection (b)(2)(F), as available.

(2) OWNERSHIP.—HA-LEU made available under this subsection—

(A) shall remain the property of, and title shall remain with, the Department; and

(B) shall not be subject to the requirements of subsection (a)(2) or (3) of the HA-LEU Act (42 U.S.C. 2013).
“(i) fuel that—

(1) directly meets the needs of the end-users described in paragraph (1); but

(2) has been previously used or fabricated for any other purpose;

(ii) fuel that can meet the needs of the end-users described in paragraph (1) after removing radioactive or other contaminants that may result from a previous use or fabrication of the fuel for research, development, demonstration, or deployment activities of the Department (including activities of the National Nuclear Security Administration);

(iii) fuel from a high-enriched uranium stockpile, which can be blended with lower assay uranium to become HA–LEU to meet the needs of the end-users described in paragraph (1); and

(iv) fuel from uranium stockpiles intended for other purposes, but for which material could be swapped or replaced in time in such a manner that would not negatively impact the missions of the Department;

(B) options for providing HA–LEU from domestically enriched HA–LEU procured by the Department through a competitive process pursuant to the HA–LEU Bank established under subsection (d)(3)(C); and

(C) options to replenish, as needed, Department stockpiles of uranium made available pursuant to subparagraph (A) with domestically enriched HA–LEU procured by the Department through a competitive process pursuant to the HA–LEU Bank established under subsection (d)(3)(C).

(5) LIMITATION. The Secretary shall not barter or otherwise sell or transfer uranium in any form in exchange for services relating to—

(A) the final disposition of radioactive waste from uranium that is the subject of a contract for sale, resale, transfer, or lease under this subsection or for

(B) environmental cleanup activities.

(6) APPROPRIATIONS.—In addition to amounts otherwise made available, there is appropriated to the Secretary to carry out this subsection, out of any amounts in the Treasury not otherwise appropriated, $150,000,000 for each of fiscal years 2022 through 2026.

(7) SUNSET.—The authority of the Secretary to carry out activities under this subsection shall terminate on the earlier of—

(A) September 30, 2027; and

(B) the date on which the HA–LEU needs of the end-users described in paragraph (1) can be fully met by commercial enrichers in the United States.

(d) COMMERCIAL HA–LEU AVAILABILITY.—

(1) ESTABLISHMENT.—Not later than 180 days after the date of enactment of this Act, the Secretary shall establish a program (referred to in this subsection as the ‘program’) to accelerate the availability of commercially produced HA–LEU in the United States in accordance with this subsection.

(2) PURPOSES.—The purposes of the program are—

(A) to provide for the availability of HA–LEU enriched, deconverted, and fabricated in the United States;

(B) to address nuclear supply chain issues in the United States; and

(C) to support strategic nuclear fuel cycle capabilities in the United States.

(3) CONSIDERATIONS.—In carrying out the program, the Secretary shall consider and, as appropriate, execute—

(A) to establish, through a competitive process, a commercial HA–LEU production capability of not less than 20 metric tons of HA–LEU per year by—

(i) not later than April 1, 2023; and

(ii) the earliest operationally feasible date thereafter; and

(B) options that provide for an array of HA–LEU—

(i) enrichment levels;

(ii) output levels to meet demand; and

(iii) fuel forms otherwise subject to the jurisdiction of, the Russian Federation or the People’s Republic of China.

(4) APPROPRIATIONS.—In addition to amounts otherwise made available, there is appropriated to the Secretary to carry out activities under subsection (c); and

(5) COST RECOVERY.—

(1) IN GENERAL.—In carrying out activities under subsections (c) and (d), the Secretary shall ensure that any HA–LEU acquired, provided, or made available under this section, out of any amounts in the Treasury not otherwise appropriated, $150,000,000 for each of fiscal years 2022 through 2026.

(2) AVAILABILITY OF CERTAIN FUNDS.—Notwithstanding subsections of this title, United States Code, revenues received from the sale or transfer of fuel feed material and other activities related to making HA–LEU available pursuant to this section, shall be subject to cost recovery in accordance with subsection (b)(2)(G).

(b)(2)(G).

(b) RETURN OR REISSUE OF EQUIPMENT RECALLED OR SEIZED PURSUANT TO REGULATIONS APPLICABLE TO DEFENSE EQUIPMENT.

It is the sense of Congress that—

(1) the signatories to the Revitalized Agreement on the Resolution of the Conflict in the Republic of South Sudan, signed on September 12, 2018, have delayed implementation, leading to continued conflict and instability in South Sudan;

(2) despite years of fighting, 2 peace agreements, punitive actions by the international community, and widespread suffering among civilian populations, the leaders of South Sudan failed to implement a credible, fair, and transparent peace;

(3) the United Nations arms embargo on South Sudan, most recently extended by 1 year to May 31, 2022, through United Nations Security Council Resolution 2578, is a necessary act by the international community to stem the illicit transfer and destabilizing accumulation and misuse of small arms and lightweight weapons in perpetuation of the conflict in South Sudan;

(4) the United States should call on other member states of the United Nations to redouble efforts to enforce the United Nations arms embargo on South Sudan; and

(5) the United States, through the United States Mission to the United Nations, should use its voice and vote in the United Nations Security Council in favor of maintaining the United Nations arms embargo on South Sudan until—

(A) the Revitalized Agreement on the Resolution of the Conflict in the Republic of South Sudan is fully implemented; or

(B) credible, fair, and transparent democratic elections are held in South Sudan.

SA 4827. MR. ROUNDS (for himself and Mr. VAN HOLLEN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, 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 of subtitile G of title XII, add the following:

SEC. 1263. SENSE OF CONGRESS ON THE NECESSITY OF MAINTAINING THE UNITED NATIONS ARMS EMBARGO ON SOUTH SUDAN UNLESS CONDITIONS FOR PEACE, STABILITY, DEMOCRACY, AND DEVELOPMENT ARE MET.

It is the sense of Congress that—

(1) the signatories to the Revitalized Agreement on the Resolution of the Conflict in the Republic of South Sudan, signed on September 12, 2018, have delayed implementation, leading to continued conflict and instability in South Sudan;

(2) despite years of fighting, 2 peace agreements, punitive actions by the international community, and widespread suffering among civilian populations, the leaders of South Sudan failed to implement a credible, fair, and transparent peace;

(3) the United Nations arms embargo on South Sudan, most recently extended by 1 year to May 31, 2022, through United Nations Security Council Resolution 2578, is a necessary act by the international community to stem the illicit transfer and destabilizing accumulation and misuse of small arms and lightweight weapons in perpetuation of the conflict in South Sudan;

(4) the United States should call on other member states of the United Nations to redouble efforts to enforce the United Nations arms embargo on South Sudan; and

(5) the United States, through the United States Mission to the United Nations, should use its voice and vote in the United Nations Security Council in favor of maintaining the United Nations arms embargo on South Sudan until—

(A) the Revitalized Agreement on the Resolution of the Conflict in the Republic of South Sudan is fully implemented; or

(B) credible, fair, and transparent democratic elections are held in South Sudan.
S5166
Congressional Record — Senate

November 18, 2021

2022 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 of subtitle B of title XII, insert the following:

SEC. 1216. STRATEGY TO SUPPORT NATIONALS OF AFGHANISTAN WHO ARE APPLICANTS FOR SPECIAL IMMIGRANT VISAS OR FOR REFERRAL TO THE UNITED STATES REFUGEE ADMISSIONS PROGRAM.

(a) Sense of Congress.—It is the sense of Congress that the United States should increase support for nationals of Afghanistan who aided the United States mission in Afghanistan during the past 20 years and are now under threat from the Taliban, specifically such nationals of Afghanistan, in Afghanistan or third countries, who are applicants for—

(1) special immigrant visas under the Afghan Allies Protection Act of 2009 (8 U.S.C. 1101 note; Public Law 111–8) or section 1059 of the National Defense Authorization Act for Fiscal Year 2016 (8 U.S.C. 1101 note; Public Law 104–163); or

(2) referral to the United States Refugee Admissions Program as refugees (as defined in section 208(a)(2)) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(2)), including as Priority 2 refugees.

(b) Strategy.—

(1) In general.—Not later than 60 days after the date of the enactment of this Act, the Secretary of State, in coordination with the Secretary of Homeland Security and the heads of other relevant Federal departments and agencies, shall submit to the appropriate committees of Congress a strategy for the safe processing abroad of nationals of Afghanistan described in subsection (a).

(2) Elements.—The strategy required by paragraph (1) shall include a detailed plan—

(A) to prioritize for evacuation from Afghanistan nationals of Afghanistan described in subsection (a);

(B) to provide for expedited initial security vetting for nationals of Afghanistan, to be conducted remotely before their departure from Afghanistan;

(C) to facilitate, after such vetting, the rapid return of Afghan nationals to their former homes or residences, or to the United States;

(D) to provide letters of support, diplomatic notes, and other documentation, as appropriate, to ease transit for such nationals of Afghanistan;

(E) to engage governments of relevant countries to better facilitate evacuation of such nationals of Afghanistan;

(F) to disseminate frequent updates to such nationals of Afghanistan and relevant nongovernmental organizations with respect to evacuation from Afghanistan;

(G) to identify and establish sufficient locations outside Afghanistan and the United States that will accept such nationals of Afghanistan during application processing (including during the processes of vetting and establishing the eligibility of such nationals of Afghanistan before their travel to the United States, which shall include any required in-person interviews) for—

(i) the special immigrant visas described in paragraph (1) of subsection (a); or

(ii) referral to the United States Refugee Admissions Program described in paragraph (2) of subsection (a);

(H) to identify necessary resources, personnel, and equipment requirements to increase capacity to better support such nationals of Afghanistan and reduce their application processing times, while ensuring strict and necessary security vetting, including, to the extent feasible, by allowing such nationals of Afghanistan to receive referrals to the United States Refugee Admissions Program while they are still in Afghanistan so as to facilitate visa processing more expeditiously; and

(I) to provide for relocation outside Afghanistan to third countries for nationals of Afghanistan described in subsection (a) who are unable to successfully complete security vetting and application processing to establish eligibility to travel to the United States.

(3) Form.—The strategy required by paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(c) Monthly Report.—

(1) In general.—Not later than 60 days after the date of the enactment of this Act, and monthly thereafter until December 31, 2022, the Secretary of State, in coordination with the Secretary of Homeland Security and the heads of other relevant Federal departments and agencies, shall submit to the appropriate committees of Congress a report on efforts to support nationals of Afghanistan described in subsection (a).

(2) Elements.—Each report required by paragraph (1) shall include the following:

(A) The number of nationals of Afghanistan referred to the United States Refugee Admissions Program as Priority 1 and Priority 2 refugees since August 29, 2021.

(B) An assessment of whether each such refugee—

(i) remains in Afghanistan; or

(ii) is outside Afghanistan;

(C) With respect to nationals of Afghanistan who have applied for referral to the United States Refugee Program, the number applications that—

(i) have been approved;

(ii) have been denied; and

(iii) are pending adjudication.

(D) The number of nationals of Afghanistan who have pending applications for special immigrant visas described in subsection (a)(1), disaggregated by special immigrant visa processing steps completed with respect to such individuals.

(E) A description of the measures taken to implement the strategy under subsection (b).

(F) The number of new congressional appropriaions for fiscal year 2022 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 of subtitle E of title X, add the following:

SEC. 1151. RELEASE OF REVOCATION INTEREST OF THE UNITED STATES IN NON-FEDERAL LAND IN SALT LAKE CITY, UTAH.

(a) Release.—There is released to the University of Utah, without consideration, the revocation interest of the United States in the non-Federal land described in subsection (b).

(b) Description of Non-Federal Land.—The non-Federal land referred to in subsection (a) is the approximately 593 acres of land of the University of Utah—

(1) depicted as “U of U Research Park” on the map—

(A) prepared by the Bureau of Land Management;

(B) entitled “University of Utah Research Park”;

(2) dated September 23, 2021;

(3) identified in the patent—

(A) numbered 43–99–6012; and

(B) dated October 18, 1968; and

(3) more particularly described as tracts D (excluding the parcels numbered 1, 2, 3, 4, and 5), G, and J, T. S. R., 1 E., Salt Lake Meridian.

SA 4380. Mr. MANCHIN (for himself, Mrs. CADDO, Mrs. HYDE-SMITH, Mr. REDDING, Mr. COTTON, Mr. COBAMUR, and Mr. TESSER) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 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 of subtitle E of title X, add the following:

SEC. 1043. HONORING HERSHEY WOODROW “WOODY” WILLIAMS AS THE LAST SURVIVING MEDAL OF HONOR RECIPIENT OF WORLD WAR II.

(a) Use of Rotunda.—Upon his death, Hershey Woodrow “Woody” Williams, who is the last surviving recipient of the Medal of Honor for acts performed in World War II, shall be permitted to lie in state in the rotunda of the United States Capitol if he or his next of kin so elects.

(b) Implementation.—The Architect of the Capitol, under the direction of the President pro tempore of the Senate and the Speaker of the House of Representatives, shall take the necessary steps to implement subsection (a).
SEC. 5102. DEFINITIONS.

In this division, unless otherwise specified:

(A) the term ‘‘agency’’ means an agency as defined in section 3552(b) of title 44, United States Code, as amended by this division.

(B) in subsection (b)(3), by inserting ‘‘security,’’ after ‘‘efficiency,’’; and

(C) in section 3533—

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

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

(1) Each agency providing a written plan under section 11331(b) shall provide any portion of the written plan addressing information security or cybersecurity to the Director of the Cybersecurity and Infrastructure Security Agency.

(b) SUBCHAPTER II DEFINITIONS.—

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

(A) by redesigning paragraphs (1), (2), (3), (4), (5), (6), (7), and (8) as paragraphs (2), (3), (4), (5), (6), (9), and (11), respectively;

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

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

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

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

(D) by adding at the end the following:

(8) ‘‘The term ‘threat hunting’ means proactively and iteratively searching for threats to systems that evade detection by automated threat detection systems.’’

(E) by adding at the end the following:

(9) ‘‘The term ‘cyber director’ means the Director of the Office of Management and Budget.’’

(F) by adding at the end the following:

(10) ‘‘The term ‘cyber director’ means the Director of the Office of Management and Budget.’’

(G) by adding the following:

(A) ‘‘The term ‘appropriate congressional committees’ means—

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

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

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

(B) in paragraph (4), by striking paragraph (3) and inserting the following:

(3) The term ‘Director’ means the Director of the Cybersecurity and Infrastructure Security Agency.”.
National Institute of Standards and Technology—

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

"(B) the use of presumption of compromise and least privilege principles to improve resilience and to respond to incidents on Federal systems.");

(C) in subsection (b)—

(i) by striking the subsection heading and inserting "CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY";

(ii) in the matter preceding paragraph (1), by striking "the Director or Secretary" and inserting "the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director and the National Cyber Director";

(iii) in paragraph (2)—

(I) in subparagraph (A)—

(aa) in clause (iii), by striking "and" and inserting "or";

(bb) in clause (iv), by adding "and" before "they", and "and" before "it";

(cc) by adding a period at the end;

(iv) in subparagraph (B), by striking "and" at the end; and

(V) by adding at the end the following:

"(E) providing an update on the ongoing and continuous assessment performed under subparagraph (A), including—

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

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

(I) the Director;

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

(III) the National Cyber Director;

(F) in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and not less frequently than once every 3 years, performing an evaluation of whether additional cybersecurity procedures determined to be appropriate to—

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

(ii) the Director; and

(iii) the National Cyber Director;

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

(H) by adding at the end the following:

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

(3) in section 3545—

(A) in subsection (a)—

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

(ii) by inserting after subparagraph (B), as so redesignated, the following:

"(A) the status of agency cybersecurity risk assessments under section 3535(a)(6);"

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

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

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

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

(vi) by striking subparagraph (C); and

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

(E) by redesignating subsections (1), (j), (k), and (l) as subsections (j), (k), (l), and (m), respectively;

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

"(1) FEDERAL RISK ASSESSMENTS.—On an ongoing and continuous basis, the Director of the Cybersecurity and Infrastructure Security Agency shall perform assessments of Federal risk posture using any available information on the cybersecurity posture of agencies, and brief the Director and National Cyber Director on the findings of those assessments including—

(I) the status of agency cybersecurity remedial actions described in section 3554(b)(7);

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

(III) analysis of incident information under section 3597;

(IV) evaluation of penetration testing performed under section 3598;

(V) evaluation of vulnerability disclosure program information under section 3598B;

(VI) evaluation of agency threat hunting results; and

(VII) evaluation of Federal and non-Federal cyber threat intelligence;"
“(II) senior agency information security officers of component agencies report to—
“(aa) the senior information security officer of the agency or an equivalent official; and
“(bb) the Chief Information Officer of the component agency or an equivalent official;”;
and
“(iv) in paragraph (5), by inserting “and the Director of the Cybersecurity and Infrastructure Security Agency” before “on the effectiveness”;

(B) in subsection (b)—

(i) by striking paragraph (1) and inserting the following:
“(1) pursuant to subsection (a)(1)(A), performing ongoing and continuous agency system risk assessments, which may include using guidelines and automated tools consistent with standards and guidelines promulgated under section 11331 of title 40, as applicable;”;

(ii) in paragraph (2)—

(I) by striking “the risk-based cyber budget model developed pursuant to section 3533(a)(7);”;

(II) in subparagraph (D)—

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

(bb) by inserting after clause (ii) the following:
“(iii) binding operational directives and emergency directives promulgated by the Director of the Cybersecurity and Infrastructure Security Agency under section 3533;”;

and

(cc) in clause (iv), as so redesignated, by striking “as determined by the agency,” and inserting “as determined by the agency, considering—

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

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

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

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

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

(vi) by inserting after paragraph (8) the following:
“(7) a process for providing the status of every remedial action and known system vulnerabilities identified to the Director and the Director of the Cybersecurity and Infrastructure Security Agency, using automation and machine-readable data to the greatest extent practicable;”;

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

(I) by striking clause (ii) and inserting the following:
“(ii) notifying and consulting with the Federal information security incident center established under section 3556 pursuant to the requirements of section 3549;”;

(II) by redesigning 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 title; and;”;

(IV) by striking “so redesignated—

(aa) in clause (I), by striking “and relevant offices of inspectors general”;

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

(cc) by striking subclause (III); and

(dd) by redesignating subclause (IV) as subclause (III)”; (C) in subsection (c)—

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

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

“(1) BIANNUAL REPORT.—Not later than 2 years after the date of enactment of the Federal Information Security Modernization Act of 2020 and not less frequently than once every 2 years thereafter, using the continuous and ongoing agency system risk assessment performed under subsection (a)(1)(A), the head of an agency, the Director of the Cybersecurity and Infrastructure Security Agency, the majority and minority leaders of the Senate, the Speaker and minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, the Committee on Commerce, Science, and Transportation of the Senate, the Committee on Science, Space, and Technology of the House of Representatives, the appropriate authorization and appropriations committees of Congress, the National Cyber Director, and the Comptroller General of the United States a report that—

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

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

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

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

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

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

“(B) may include a classified annex.

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

“(4) BRIEFCING.—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 “so redesignated—

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

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

(cc) by striking subclause (III); and

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

(B) in subsection (a)—

(i) in paragraph (1), by inserting “during which a report is required to be submitted under section 3533(c)” after “Each year”;

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

(iii) by adding at the end the following:

“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 3533(c)” after “Each year”;

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

“(1) IN SUBSECTION OF INFORMATION.—(I) Agencies, evaluators, and other recipients of information that, if disclosed, may cause grave harm to the efforts of Federal information security officers to take appropriate steps to ensure the protection of that information, including safeguarding the information from unauthorized disclosure.

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

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

“(A) specific information system incidents; or

“(B) specific information system vulnerabilities.”;

(F) in subsection (g)(2)—

(i) by striking “this subsection shall” and inserting “this subsection—

“(A) shall”;

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

and

(iii) by adding at the end the following:

“(B) identify any entity that performs an independent evaluation under subsection (b);”;

and

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

“(j) GUIDANCE.—

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

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

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

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

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

and

(i) in section 3556(a)—

(A) in the matter preceding paragraph (1), by inserting “within the Cybersecurity and Infrastructure Security Agency” after “including”; and

(B) in paragraph (4), by striking “3556(b)” and inserting “3554(a)(1)(A)”.

S8519
CONGRESSIONAL RECORD — SENATE November 18, 2021

S5520

(d) CONFORMING AMENDMENTS.—

(1) TABLE OF SECTIONS.—The table of sections for chapter 35 of title 44, United States Code, is amended—

(A) by inserting before the item relating to section 3553 and inserting the following:

"3553. Authority and functions of the Director and the Director of the Cybersecurity and Infrastructure Security Agency;" and

(B) 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 (5 U.S.C. 5726(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 3555(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. 3703(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 3502 shall apply to this chapter.

(b) APPROPRIATE REPORTING ENTITIES.—As used in this subchapter:

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

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

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

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

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

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

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

(G) the Director;

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

(I) the National Cyber Director;

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

(K) the inspector general of any impacted agency.

(2) AWARDEE.—The term 'awardee' means—

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

(B) any person or business that collects or maintains information, including personally identifiable information, on behalf of an agency.

(3) 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.

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

(5) 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).

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

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

§ 3592. Notification of breach

(a) Notification.—An exegiendum as practicable and without unreasonable delay, and in any case not later than 45 days after an agency has a reasonable basis to conclude that a breach has occurred, the head of the agency, in consultation with a senior privacy officer of the agency, shall—

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

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

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

(C) the type of breach; and

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

(2) as appropriate, provide written notice in accordance with subsection (b) to each individual potentially affected by the breach—

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

(B) through an alternative method of notification that the head of the agency or a designated senior-level individual of the agency selects based on factors determined by the Director.

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

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

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

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

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

(B) may include a telephone number or a website;

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

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

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

(c) DELAY OF NOTIFICATION.—

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

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

(B) reveal sensitive systems and methods;

(C) cause damage to national security; or

(D) hamper security remediation actions.

(2) DOCUMENTATION.—

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

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

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

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

(5) EXEMPTION FROM NOTIFICATION.—

(1) IN GENERAL.—The head of an agency, in consultation with the inspector general of the agency, may request an exemption from the Director from complying with the notification requirements under subsection (a) if the Director determines there is a significant change in the reasonable basis to conclude that a breach occurred, a significant change to the determination made under subsection (a), or that it is necessary to update the details of the information provided to impacted individuals as described in subsection (b), the agency shall as expeditiously as practicable and without unreasonable delay, and in any case not later than 30 days after such a determination, notify each individual who received a notification pursuant to subsection (a) of those changes.

(6) DOCUMENTATION.—

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

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

(1) the Director from issuing guidance relating to notifications or the head of an agency that experienced a breach.
agency from notifying individuals potentially affected by breaches that are not determined to be major incidents; or
(2) the Director from issuing guidance relating to notifications of major incidents or the head of an agency from providing more information than described in subsection (b) when notifying individuals potentially affected by a major incident.

§ 3593. Congressional and Executive Branch reports
(a) Initial Report.—
(1) In general.—Not later than 72 hours after an agency has a reasonable basis to conclude that a major incident occurred, the head of the agency impacted by the major incident shall submit to the appropriate reporting entity a written report and, to the extent practicable, provide a briefing to the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, and the appropriate authorization and appropriations committees of Congress, taking into account—
(A) the information known at the time of the report;
(B) the sensitivity of the details associated with the major incident; and
(C) the classification level of the information contained in the report.

(b) Report required under paragraph (1) shall include, in a manner that excludes or otherwise reasonably protects personally identifiable information and to the extent practicable, provide any information available to applicable law, including privacy and statistical laws—
(A) a summary of the information available about the major incident, including how the major incident occurred, information indicating that the major incident may be a breach, and information relating to the major incident as a breach, based on information available to agency officials as of the date on which the agency submits the report;
(B) if applicable, a description and any associated documentation of any circumstances necessitating a delay in or exception to notification to individuals potentially affected by the major incident under subsection (c) or (e) of section 3592; and
(C) if applicable, an assessment of the impact to the agency, the Federal Government, or the security of the United States, based on information available to agency officials on the date on which the agency submits the report.

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

(d) Components.—The briefing required under paragraph (1) shall include the greatest extent practicable, include an unclassified component; and
(B) may include a classified component.

(e) Rule of Construction.—Nothing in this section shall be construed to limit—
(1) the ability of an agency to provide additional reports or briefings to Congress;
(2) Congress from requesting additional information from agencies through reports, briefings, or other means.

§ 3594. Government information sharing and incident response
(a) In general.—
(1) Incident Reporting.—The head of each agency shall provide any information relating to any incident to any agency as defined by the Director and not involving national security, privacy, statistical confidentiality, or other factors determined by the Director in order to protect against a similar incident.

(b) whether the agency implemented the safeguards described in subparagraph (A) correctly;
(C) in order to protect against a similar incident;
(1) how the safeguards described in subparagraph (A) should be implemented differently;
and
(2) additional necessary safeguards; and
(D) include information to aid in incident response, such as—
(i) a description of the affected systems or network;
(ii) the estimated dates of when the incident occurred; and
(iii) information that could reasonably help identify the party that conducted the incident.

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

(4) National Security Systems.—Each agency operating or exercising control of a national security system shall share information about incidents that occur on national security systems with the Director of the Cybersecurity and Infrastructure Security Agency to the extent consistent with standards and guidelines for national security systems issued in accordance with law and as directed by the President.

(b) Compliance.—The information provided under subsection (a) shall take into account the level of classification of the information and any information sharing limitations and protections, such as limitations and protections relating to law enforcement, national security, privacy, statistical confidentiality, or other factors determined by the Director.

(c) Incident Response.—Each agency that has a reasonable basis to conclude that a major incident occurred involving Federal information in electronic medium or form, as defined by the Director and not involving a national security system, regardless of delays from notification granted for a major incident, shall coordinate with the Cybersecurity and Infrastructure Security Agency regarding—
(1) incident response and recovery; and
(2) recommendations for mitigating future incidents.

§ 3595. Responsibilities of contractors and awardees
(a) Notification.—
(1) In general.—Unless otherwise specified in the contract, grant, cooperative agreement, or other transaction agreement, any contractor or awardee of an agency shall report to the agency within the same amount of time such agency is required to report an incident to the Cybersecurity and Infrastructure Security Agency, if the contractor or awardee has a reasonable basis to conclude that—
(A) an incident or breach has occurred with respect to Federal information collected, used, or maintained by the contractor or awardee in connection with the performance of the contract, grant, cooperative agreement, or other transaction agreement of the contractor or awardee;
(B) the incident or breach has occurred with respect to a Federal information system used or operated by the contractor or awardee in connection with the contract, grant, cooperative agreement, or other transaction agreement of the contractor or awardee;
(C) the contractor or awardee has received information from the agency that the contractor or awardee is not authorized to receive in connection with the contract,
(2) Proceedings.—

(A) MAJOR INCIDENT.—Following a report of a breach or major incident by a contractor or awardee under paragraph (1), the agency, in consultation with the contractor or awardee, shall carry out the requirements under sections 3592, 3593, and 3594 with respect to the major incident.

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

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

§ 3596. Training

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

(b) REQUIREMENT.—The head of each agency shall develop training for covered individuals on system security and respond to an incident, including—

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

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

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

§ 3597. Analysis and report on Federal incidents

(a) ANALYSIS OF FEDERAL INCIDENTS.—

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

(A) incidents, including—

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

(ii) system vulnerabilities, including zero day vulnerabilities, and information system misconfigurations;

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

(C) cross Federal Government root causes of incidents at agencies;

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

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

(F) trends in cross-Federal Government 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)).

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

(3) SHARING OF DATA AND ANALYSIS.—

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

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

(ii) support the cybersecurity improvement efforts of agencies.

(B) FORMING CARRYING OUT SUBPARAGRAPH (A), the Director shall share the analyses—

(i) in human-readable written products; and

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

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

(1) a summary of causes of incidents from across the Federal Government that categorizes those incidents as major 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 response to breaches, including—

(i) the information described in subparagraph (A); and

(ii) 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 compromises 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)).

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

(d) INFORMATION PROVIDED BY AGENCIES.—

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

(2) NONCOMPLIANCE REPORTS.—

(A) IN GENERAL.—Subject to subparagraph (B), during any year during which the head of an agency does not provide data for an incident, the Director of the Cybersecurity and Infrastructure Security Agency and the Director, shall submit to the appropriate reporting entities a report that includes—

(i) data for the incident; and

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

(B) EXCEPTION FOR NATIONAL SECURITY SYSTEMS.—The head of an agency that owns or exercises control of a national security system shall not include data for an incident that occurs on a national security system in any report submitted under subparagraph (A).

(3) NATIONAL SECURITY SYSTEM REPORTS.—

(A) IN GENERAL.—Annually, the head of an agency that owns or exercises control of a national security system shall submit a report that includes the information described in subsection (b) with respect to the agency, and the report is consistent with standards and guidelines for national security systems issued in accordance with law and as directed by the President to—

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

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

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

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

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

(vi) the Committee on Appropriations of the Senate;

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

(viii) the Committee on Homeland Security and Governmental Affairs of the House of Representatives;

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

(x) the House of Representatives.

(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 system operated or maintained by or on behalf of an agency or an information system used or operated by an agency or by a contractor of an agency or another organization on behalf of an agency, the term ‘major incident’ to the purposes of subchapter II and this subchapter.

(c) REPORT.—With respect to the guidance issued under subsection (a), the definition of the term ‘major incident’ shall—

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

(ii) the civil liberties or public health and safety of the people of the United States.

(3) any incident that the head of the agency determines likely to result in an inability for the agency, a component of the agency, or the Federal Government, to provide 1 or more critical services.

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

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

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

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

(G) any incident involving the exposure of sensitive agency information to a foreign entity.

(H) any incident involving the exposure of sensitive agency information to a foreign entity.

(I) any incident involving the exposure of sensitive agency information to a foreign entity.

(J) any incident involving the exposure of sensitive agency information to a foreign entity.

(K) any incident involving the exposure of sensitive agency information to a foreign entity.

(L) any incident involving the exposure of sensitive agency information to a foreign entity.

(M) any incident involving the exposure of sensitive agency information to a foreign entity.

(N) any incident involving the exposure of sensitive agency information to a foreign entity.

(O) any incident involving the exposure of sensitive agency information to a foreign entity.

(P) any incident involving the exposure of sensitive agency information to a foreign entity.

(Q) any incident involving the exposure of sensitive agency information to a foreign entity.

(R) any incident involving the exposure of sensitive agency information to a foreign entity.

(S) any incident involving the exposure of sensitive agency information to a foreign entity.

(T) any incident involving the exposure of sensitive agency information to a foreign entity.

(U) any incident involving the exposure of sensitive agency information to a foreign entity.

(V) any incident involving the exposure of sensitive agency information to a foreign entity.

(W) any incident involving the exposure of sensitive agency information to a foreign entity.

(X) any incident involving the exposure of sensitive agency information to a foreign entity.

(Y) any incident involving the exposure of sensitive agency information to a foreign entity.

(Z) any incident involving the exposure of sensitive agency information to a foreign entity.
of the agency or the head of a component of the agency; and

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

(’H) any incident described in paragraph (1) of the National Cyber Director shall declare a major incident at each agency impacted by an incident if the Director of the Cybersecurity and Infrastructure Security Agency determines that an incident—

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

(’B) is enabled by—

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

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

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

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

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

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

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

(ii) the Chair of the Federal Trade Commission.

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

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

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

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

(’A) an update, if necessary, to the guidance in subsection (a); and

(’B) 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. Govt. Infor. system sharing and incident response.

3595. Responsibilities of contractors and awardees.

3596. Training.


3598. Major incident definition.’’.

SEC. 512. AMENDMENTS TO SUBTITLE III OF TITLE 40.


(1) in section 1077(b)—

(A) in paragraph (5)(A), by inserting ‘‘improving the cybersecurity of systems and before ‘cost savings activities’’;

(B) in paragraph (6)(A)—

(i) in the paragraph heading, by striking ‘‘cio’’ and inserting ‘‘CIO’’;

(ii) by striking ‘‘in evaluating projects’’ and inserting ‘‘and Infrastructure Security Agency’’;

(2) in section 1078—

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

(’a) DEFINITIONS.—In this section:

(i) Agency.—The term ‘agency’ has the meaning given in title 5 of United States Code.

(ii) High value asset.—The term ‘high value asset’ has the meaning given in the term in section 3552 of title 44, United States Code.

(B) in section 1079—

(i) in subsection (a), by striking ‘‘and performance’’ and inserting ‘‘including cybersecurity performance’’;

(ii) in subsection (b), by inserting ‘‘including cybersecurity performance’’.

(c) Application of More Stringent Standards.—

(1) In general.—The head of an agency shall—

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

(2) to the greatest extent practicable and if it is determined after application of an applicable standard that necessary, employ those standards.

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

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

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

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

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

(4) AUTOMATED STANDARD IMPLEMENTATION SECURITY现代化 Act of 2014.

SEC. 512. ACTIONS TO ENHANCE FEDERAL INCIDENT RESPONSE.

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

(I) a description of any challenges the Director anticipates encountering; and

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

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

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


(A) by striking subsection (b); and

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

(2) INCIDENT DATA SHARING.—

(A) IN GENERAL.—The Director shall develop guidance, to be updated not less frequently than once every 2 years, for use by Federal agencies of incident reports, content, timelines, and format of the information provided by agencies under section 3595 of title 44, United States Code, as added by this division.

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

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

(I) the causes of incidents; and

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

(II) a root cause analysis of incidents that—

(aa) are common across the Federal Government; or

(bb) have a Government-wide impact;

(iii) agency response, recovery, and remediation actions; and

(V) the impact of incidents; and

(ii) enable the efficient development of—

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

(ii) the report on Federal incidents required under section 3595(b) of title 44, United States Code, as added by this division;

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

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

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

(d) STANDARD GUIDANCE AND TEMPLATES.—Not later than 1 year after the date of enactment of this Act, the Director, in coordination with the Secretary of Homeland Security, the Secretary of Defense, the Administrator of General Services, and the heads of other agencies determined appropriate by the Director, shall issue guidance to Federal agencies on how to deconflict, to the greatest extent practicable, existing regulations, policies, and procedures relating to the responsibilities of contractors and awardees established under section 3595 of title 44, United States Code, as added by this division.

(e) EXISTING PROCESSES.—To the greatest extent practicable, the guidance issued under subsection (a) shall allow contractors and awardees to use existing processes notifying Federal agencies of incidents involving information of the Federal Government.
(6) UPDATED BRIEFINGS.—Not less frequently than once every 2 years, the Director shall provide to the appropriate congressional committees an update on the guidance and the progress developed under subparagraphs (2) through (4).

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

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

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

(3) by adding at the end the following:

'(13) to another agency in furtherance of a responsibility assigned to it under section 3532 of title 44 and pursuant to the information sharing requirements in section 3594 of title 44 if the head of the requesting agency has made a written request to the agency that maintains the record specifying the particular portion desired and the activity for which the record is sought.'.

SEC. 5124. ADDITIONAL GUIDANCE TO AGENCIES ON FISMA UPDATES.

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

(1) providing 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 division;

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

(3) establishing a process for providing the status of each remedial action under section 3554(b)(7) of title 44 if the head of the requesting agency has made a written request to the agency that maintains the record specifying the particular portion desired and the activity for which the record is sought;

(4) through (4).

(a) DEFINITIONS.—In this section:

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

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

(2) interpreting the definition of ‘‘high value asset’’ under section 3532 of title 44, United States Code, as amended by this division;

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

SEC. 5125. 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) SECURITY INFORMATION.—The term ‘‘sensitive information’’ means the sensitive information that is submitted by the Director in guidance issued under subsection (b).

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

(1) the confidentiality or integrity of sensitive information or of the systems used in the transmission or storage of the sensitive information described in paragraph (1).

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

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

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

(3) a requirement for every agency to provide to the appropriate congressional committees a briefing on the guidance.

SEC. 5126. DATA AND LOGGING RETENTION FOR INCIDENT RESPONSE.

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

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

(1) the types of logs to be maintained;

(2) the time periods to retain the logs and other relevant data;

(3) the time periods for agencies to enable recommended logging and security requirements;

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

(5) requirements to ensure that, upon request, in a manner that excludes or otherwise reasonably protects personally identifiable information, and to the extent permitted by applicable law (including privacy and statistical laws), agencies provide logs to—

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

(B) the Federal Bureau of Investigation to investigate potential criminal activity; and

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

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

SEC. 5141. CISA AGENCY ADVISORS.

(a) IN GENERAL.—Not later than 120 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall assign not less than 2 cybersecurity professionals, employed by the Cybersecurity and Infrastructure Security Agency to be the Cybersecurity and Infrastructure Security Agency advisor to the senior agency information security officer of each agency.

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

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

(2) performing risk assessments of agency systems; and

(3) other Federal cybersecurity initiatives.

(c) QUALIFICATIONS.—The advisor assigned under subsection (a) shall include—

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

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

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

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

(e) MULTIPLE ASSIGNMENTS.—One individual advisor may be assigned to multiple agencies.

SEC. 5144. PENETRATION TESTING POLICY.

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

‘‘§ 3559A. Federal penetration testing

‘‘(a) DEFINITIONS.—In this section:

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

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

'(b) GUIDANCE.—

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

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

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

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

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

'(A) a shared service of the agency or another agency; or

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

'(3) require agencies to provide the rules of engagement and results of penetration testing to the Director and the Director of the Cybersecurity and Infrastructure Security Agency, or any other appropriate entity, without regard to the status of the entity that performs the penetration testing.

November 18, 2021

CONGRESSIONAL RECORD — SENATE

S8525
``(c) AGENCY PLANS AND RULES OF ENGAGEMENT.—The agency operational plan and rules of engagement of an agency shall—

(1) require the agency to—

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

(B) coordinate with the Director of the Cybersecurity and Infrastructure Security Agency pursuant to section 3559A that penetration testing is being performed;

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

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

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

(C) uses as data to data;

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

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

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

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

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

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

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

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

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

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

(f) PRIORITY OF PENETRATION TESTING RESOURCES.—

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

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

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

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

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

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

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

(h) DELIGATION OF AUTHORITY FOR CERTAIN INTELLIGENCE.—The authorities of the Director described in subsection (b) shall be delegated—

(1) to the Secretary of Defense in the case of military intelligence in the case of systems described in section 3555(e)(3).; and

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

``

(b) FRAMEWORK FOR GUIDANCE.—Not later than 180 days after the date of enactment of this Act, the Director shall issue the guidance required under section 3550A(b) of title 44, United States Code, as added by subsection (a).

(c) CLERICAL AMENDMENT.—The table of sections 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 section 5121, is further amended—

(1) in paragraph (8)(B), by striking ‘‘and’’ at the end;

(2) by redesignating paragraph (9) as paragraph (8); and

(3) by inserting after paragraph (8) the following:

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

SEC. 5145. ONGOING THREAT HUNTING PROGRAM.

(a) THREAT HUNTING PROGRAM.—

(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 establish a program to provide ongoing, hypothesis-driven threat-hunting services on the network of each agency.

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

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

(B) provide on-premises support to agencies;

(C) staff threat hunting services;

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

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

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

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

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

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

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

(3) not later than 1 year after the date on which the Director of the Cybersecurity and Infrastructure Security Agency provides threat hunting services under the program established under this section, a report describing lessons learned from providing those services.

SEC. 5146. CODIFYING VULNERABILITY DISCLOSURE PROGRAMS.

(a) DEFINITIONS.—In this section:

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

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

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

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

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

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

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

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

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

(D) any other information with respect to which the head of the agency determines that an examination necessary to the Cybersecurity and Infrastructure Security Agency.

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

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

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

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

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

(d) RESPONSIBILITIES OF AGENCIES.—

(1) PURCHASE INFORMATION.—The head of each agency shall purchase, to the extent practicable, information from a contractor, as defined in section 7013 of title 40, United States Code, for the purpose of protecting agency systems.

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

(A) describe—

(i) the scope of the systems of the agency included in the vulnerability disclosure policy;
(ii) the type of information system testing that is authorized by the agency;
(iii) the information system testing that is not authorized by the agency; and
(iv) the disclosure policy of the agency for sensitive information;

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

(i) how the reporter should submit the report; and

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

(C) include any other relevant information; and

(D) be mature in scope, to cover all Federal information systems used or operated by that agency or on behalf of that agency.

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

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

(f) CONGRESSIONAL REPORTING.—Not later than 90 days after the date of enactment of the Federal Information Security Modernization Act of 2021, and annually thereafter for a 5-year period thereafter, the Director shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives a briefing on the status of the use of vulnerability disclosure policies under this section at agencies, including, with respect to the guidance issued under subsection (a)(1), an identification of the agencies that are compliant and not compliant.

(g) EXEMPTIONS.—The authorities and functions of the Director and the Director of the Cybersecurity and Infrastructure Security Agency under this section shall not apply to national intelligence agencies.

(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 3555(e)(2); and

(2) to the Director of National Intelligence in the case of systems described in section 3555(e)(3).

(2) CLINICAL AMENDMENT.—The table of sections for chapter 35 of title 44, United States Code, is amended by adding after the item relating to section 355A, as added by section 355B of this Act, the following:

"359B. Federal vulnerability disclosure programs.".

SEC. 5147. IMPLEMENTING PRESUMPTION OF COMPROMISE AND LEAST PRIVILEGE PRINCIPLES.

(a) GUIDANCE.—Not later than 1 year after the date of enactment of this Act, the Director shall provide an update to the appropriate congressional committees on progress in increasing the internal defenses of agency systems, including—

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

(2) reviewing the 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 deauthorizing unauthorized entities from agency systems quickly;

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

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

(b) AGENCY PROGRESS REPORTS.—Not later than 1 year after the date of enactment of this Act, the head of each agency shall submit to the Director a progress report on implementing an information security program based on the presumption of compromise and least privilege principles, which shall include—

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

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

(3) a schedule to implement any planned activities.

SEC. 5148. AUTOMATION REPORTS.

(a) OMB REPORT.—Not later than 180 days after the date of enactment of this Act, the Director shall submit to Congress a report on the utility of the covered metrics included in guidance issued under paragraph (1) and any subsequent guidance that requires agencies to share with the Director of the Cybersecurity and Infrastructure Security Agency data demonstrating the performance of the agency using the covered metrics included in the guidance.

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

(c) IMPROVEMENT METRICS.—"(1) IN GENERAL.—The Director of the Cybersecurity and Infrastructure Security Agency shall develop a capability that allows for the analysis of the covered metrics, including cross-agency performance of agency cybersecurity and incident response capabilities.

(2) QUALITIES.—With respect to the metrics established, reviewed, and updated under paragraph (1), the Director shall ensure that the metrics—

(i) the detection of an incident and the remediation of the incident; and

(ii) the amount of time that passes between the detection of an incident and the remediation of the incident; and

(3) PENETRATION TESTS.—On not less than 2 occasions during the 2-year period following the date on which guidance is promulgated under paragraph (1), the Director shall ensure that not less than 3 agencies are subjected to substantially similar penetration tests, as determined by the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, in order to validate the utility of the covered metrics.

SEC. 5149. EXTENSION OF FEDERAL ACQUISITION SECURITY COUNCIL.

Section 1328 of title 41, United States Code, is amended by striking "the date that" and all that follows and inserting "December 31, 2026."

SEC. 5150. COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY DASHBOARD.

(a) DASHBOARD REQUIRED.—Section 11(e)(2) of the Inspector General Act of 1978 (5 U.S.C. App. 1) is amended—

(1) by striking subsection (e); and

(2) by inserting after subparagraph (C) the following:

"(D) that shall include a dashboard of open information security recommendations identified in the independent evaluations required by section 3555(a) of title 44, United States Code; and"

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

(c) IMPROVED METRICS.—"(1) IN GENERAL.—The Director of the Cybersecurity and Infrastructure Security Agency shall establish, review, and update metrics to measure the cybersecurity and incident response capabilities of agencies in accordance with the responsibilities of agencies under section 3554 of title 44, United States Code.

(2) QUALITIES.—With respect to the metrics established, reviewed, and updated under paragraph (1)—

(i) the amount of time that passes between the detection of an incident and the remediation of the incident; and

(ii) the amount of time that passes between the detection of an incident and the recovery from the incident; and

(iii) the metrics may include or measurable outcomes;"

(d) CONGRESSIONAL REPORTS.—The Inspectors General of the respective agencies shall submit to the appropriate congressional committees a report on the utility of the covered metrics.

(e) CYBERSECURITY ACT OF 2015 UPDATES.—Section 224 of the Cybersecurity Act of 2015 (6 U.S.C. 1522) is amended—

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

"(c) CYBERSECURITY METRICS.—"(1) IN GENERAL.—The Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Director, shall establish, review, and update metrics to measure the cybersecurity and incident response capabilities of agencies in accordance with the responsibilities of agencies under section 3554 of title 44, United States Code.

(2) QUALITIES.—With respect to the metrics established, reviewed, and updated under paragraph (1)—

(i) the amount of time that passes between the detection of an incident and the remediation of the incident; and

(ii) the amount of time that passes between the detection of an incident and the recovery from the incident; and

(iii) the metrics may include or measurable outcomes;"

(f) CONGRESSIONAL REPORTS.—The Inspectors General of the respective agencies shall submit to the appropriate congressional committees a report on the utility of the covered metrics.

(g) CYBERSECURITY METRICS.—Section 3554(b) of title 44, United States Code, is amended—

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

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

(h) CONGRESSIONAL REPORTS.—The Inspectors General of the respective agencies shall submit to the appropriate congressional committees a report on the utility of the covered metrics.
(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ‘‘appropriate congressional committees’’ means—
(A) the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate; and
(B) the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives.

(2) COVERED AGENCY.—The term ‘‘covered agency’’ has the meaning given the term ‘‘executive agency’’ in section 135 of title 41, United States Code.

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

(4) INFORMATION TECHNOLOGY.—The term ‘‘information technology’’—
(A) has the meaning given the term in section 1105 of title 41, United States Code; and
(B) includes the hardware and software systems of a Federal agency that monitor and control physical equipment and processes of the Federal agency.

(5) RISK-BASED BUDGET.—The term ‘‘risk-based budget’’ means a budget—
(A) developed by identifying and prioritizing cybersecurity risks and vulnerabilities, including impact on agency operations in the case of a cyber attack, through analysis of cyber threat intelligence, and tactics, techniques, procedures, and capabilities of cyber threats; and
(B) that allocates resources based on the risks identified and prioritized under subparagraph (A).

SEC. 5162. ESTABLISHMENT OF RISK-BASED BUDGET MODEL.

(a) IN GENERAL.—
(1) MODEL.—Not later than 1 year after the first publication of the budget submitted by the President, as defined in section 3553(a)(2) of title 44, United States Code, following the date of enactment of this Act, the Director shall submit a report to Congress on the development of the model required under section 3554(d)(2) of title 44, United States Code, as amended by subsection (b), the risk-based budget model for cybersecurity spending.

(2) RESPONSIBILITY OF DIRECTOR.—Section 3554(a)(2) of title 44, United States Code, as amended by section 5121 of this division, is further amended by inserting after paragraph (6) the following:

‘‘(7) developing an standard risk-based budget model to inform Federal agency cybersecurity budget development; and’’.

(3) CONTENTS OF MODEL.—The model required to be developed under paragraph (1) shall—
(A) consider Federal and non-Federal cyber threat intelligence products, where available, to identify threats, vulnerabilities, and risks;
(B) consider the impact of agency operations of compromise of systems, including the impact of threats to other agency systems and the operations of other agencies;
(C) indicate where resources should be allocated to have the greatest impact on mitigating current and future threats and current and future cybersecurity capabilities;
(D) be used to inform acquisition and sustainment of—
(i) information technology and cybersecurity tools;
(ii) information technology and cybersecurity architectures;
(iii) information technology and cybersecurity personnel; and
(iv) cybersecurity and information technology concepts of operations; and
(E) be made available to and inform Government-wide cybersecurity programs of the Department of Homeland Security.

(b) REQUIRED USE OF RISK-BASED BUDGET MODEL.—
(1) IN GENERAL.—Not later than 2 years after the date on which the model developed under subsection (a) is published, the head of each covered agency shall use the model to develop the annual cybersecurity and information technology budget requests of the agency.

(2) AGENCY PERFORMANCE PLANS.—Section 3554(d)(2) of title 44, United States Code, is amended by inserting ‘‘and the risk-based budget model required under subsection (a)(7)’’ after ‘‘paragraph (1)’’.

(c) VERIFICATION.—
(1) INDEPENDENT EVALUATION.—Section 1105(a)(35)(A)(1) of title 31, United States Code, is amended—
(A) in the matter preceding subclause (I), by striking ‘‘by agency, and by initiative area (as determined by the administration)’’ and inserting ‘‘and by agency’’;
(B) in subparagraph (B), by striking ‘‘and’’ at the end; and
(C) by adding at the end the following:

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

(VI) a report on the progress of each agency on closing recommendations identified under the independent evaluation required by section 3555(a)(1) of title 44.’’

(2) EFFECTIVE DATE.—The amendments made by paragraph (1) shall take effect on the date that is 2 years after the date on which the model developed under subsection (a) is published.

(d) REPORTS.—
(1) INDEPENDENT EVALUATION.—Section 3555(a)(2) of title 44, United States Code, is amended—
(A) in subparagraph (B), by striking ‘‘and’’ at the end;
(B) in subparagraph (C), by striking the period at the end and inserting ‘‘and’’; and
(C) by adding at the end the following:

‘‘(D) an assessment of how the agency implemented the risk-based budget model required under subsection (a); and

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

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

(G) a report on the progress of each agency on closing recommendations identified under the independent evaluation required by section 3555(a)(1) of title 44.’’

(2) EFFECTIVE DATE.—The amendments made by paragraph (1) shall take effect on the date that is 2 years after the date on which the model developed under subsection (a) is published.

(e) GAO REPORT.—Not later than 3 years after the date of enactment of this Act, and annually thereafter for each of the 2 following fiscal years or until the date on which the model required to be developed under subsection (a) is published, whichever is sooner, the Director shall submit a report to Congress on the development of the model.

SEC. 5181. ACTIVE CYBER DEFENSIVE STUDY.

(a) DEFINITION.—In this section, the term ‘‘active defense technique’’ means—
(1) an action taken on the systems of an entity to increase the security of information on the network of an agency by misleading an adversary; and
(2) includes a honeypot, deception, or purposefully feeding false or misleading data to an adversary when the adversary is on the systems of the entity.

(b) STUDY.—Not later than 180 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall develop a plan to implement active defense techniques designed to support the cybersecurity and information technology budget requests of the agency.

(c) CONTENTS.—The plan required under subsection (b) shall include—
(1) a review of legal restrictions on the use of different active defense techniques in Federal environments, in consultation with the Department of Justice;
(2) an evaluation of—
(A) the efficacy of a selection of active defense techniques determined by the Director of the Cybersecurity and Infrastructure Security Agency; and
(B) factors that impact the efficacy of the active defense techniques evaluated under paragraph (A);
(3) recommendations on safeguards and procedures that shall be established to require that active defense techniques are adequately coordinated to ensure that active defense techniques do not impact the threat response efforts, criminal investigations, and national security activities, including intelligence collection; and
(4) the development of a framework for the use of different active defense techniques by agencies.

SEC. 5182. SECURITY OPERATIONS CENTER AS A SERVICE PILOT.

(a) PURPOSE.—The purpose of this section is for the Cybersecurity and Infrastructure Security Agency to run a security operations center on behalf of another agency, alleviating the need to duplicate this function at every agency, and empowering a greater centralized cybersecurity capability.

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

(c) CONTENTS.—The plan required under subsection (b) shall include considerations for—
(1) collecting, organizing, and analyzing agency information system data in real time;
(2) staffing and resources; and
(3) appropriate interagency agreements, concepts of operations, and governance plans.
(d) Pilot Program.—
(1) IN GENERAL.—Not later than 180 days after the date on which the plan required under subsection (b) is developed, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director, shall enter into a 1-year agreement with not less than 2 agencies to offer a security vulnerability disclosure program on a shared services basis.

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

(e) BRIEFING AND REPORT.—
(1) BRIEFING.—Not later than 360 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Oversight and Reform of the House of Representatives a briefing on the parameters of any 1-year agreements entered into under subsection (d).

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

DIVISION F—CYBER INCIDENT REPORTING ACT OF 2021 AND CISA TECHNICAL SECURITY CONTROLS FOR AGENCIES AND IMPROVEMENTS ACT OF 2021

TITLE LXI—CYBER INCIDENT REPORTING ACT OF 2021

SEC. 6101. SHORT TITLE. This title may be cited as the “Cyber Incident Reporting Act of 2021”.

SEC. 6102. DEFINITIONS. In this title:

(1) COVERED CYBER INCIDENT; COVERED ENTITY; CYBER INCIDENT.—The terms “covered cyber incident”, “covered entity”, and “cyber incident” have the meanings given those terms in section 2230 of the Homeland Security Act of 2002, as added by section 6103 of this title.

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

(3) INFORMATION SYSTEM; RANSOMWARE PAYMENT; RANSOMWARE ATTACK; SECURITY VULNERABILITY.—The terms “information system”, “ransomware payment”, “ransomware attack”, and “security vulnerability” have the meanings given those terms in section 2200 of the Homeland Security Act of 2002, as added by section 6103 of this title.

SEC. 6103. CYBER INCIDENT REPORTING.

(a) CYBER INCIDENT REPORTING.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—
(1) by adding at the end the following:

“Subtitle C—Cyber Incident Reporting

SEC. 2230. DEFINITIONS.

“In this subtitle:

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

(2) COUNCIL.—The term ‘Council’ means the Cyber Incident Reporting Council described in section 1702(c)(1)(B) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)).

(3) COVERED CYBER INCIDENT.—The term ‘covered cyber incident’ means a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the final rule issued pursuant to section 2232(b).

(4) COVERED ENTITY.—The term ‘covered entity’ means—
(A) any Federal contractor; or
(B) an entity that owns or operates critical infrastructure that satisfies the definition established by the Director in the final rule issued pursuant to section 2232(b).

(5) CYBER INCIDENT.—The term ‘cyber incident’ has the meaning given the term ‘incident’ in section 2230.

(6) CYBER THREAT.—The term ‘cyber threat’—
(A) has the meaning given the term ‘cybersecurity threat’ in section 2200; and
(B) does not include any activity related to good faith security research, including participation in a bug-bounty program or a vulnerability disclosure program.

(7) FEDERAL CONTRACTOR.—The term ‘Federal contractor’ means—
(A) a service contract to provide housekeeping or custodial services; or
(B) a contract to provide products or services unrelated to information technology that satisfies the definition and criteria established by the Director in the final rule issued pursuant to section 2232(b).

(8) FEDERAL ENTITY; INFORMATION SYSTEM; SECURITY CONTROL.—The term ‘Federal entity’ means—
(A) a service contract to provide housekeeping or custodial services; or
(B) a contract to provide products or services unrelated to information technology that satisfies the definition and criteria established by the Director in the final rule issued pursuant to section 2232(b).

(9) SIGNIFICANT CYBER INCIDENT.—The term ‘significant cyber incident’ means a cybersecurity incident, or a group of cybersecurity incidents, that together satisfy such definition, contain a covered cyber incident or group of those incidents that together satisfy such definition, constitute a covered cyber incident, or group of those incidents, that together satisfy such definition, and constitute a cybersecurity incident, or group of those incidents, that together satisfy such definition, and have a substantial cyber threat, and together with ransom payments, particularly with respect to ransom payments, in a manner that compromises the security of the information systems and networks of United States government agencies, to support law enforcement investigations, to assess potential impact of incidents on public health and safety, and to have a more accurate picture of the cyber threat to critical infrastructure and the people of the United States;

(10) SMALL ORGANIZATION.—The term ‘small organization’ means—
(A) a business, nonprofit organization, or other private sector entity that is a covered entity; or
(B) a Federal contractor.

SEC. 2231. CYBER INCIDENT REVIEW.

(1) ACTIVITIES.—The Council shall—
(A) receive, aggregate, analyze, and secure reports that lead to the identification of tactics, techniques, and procedures used to perpetrate cyber incidents and ransomware attacks;

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

(C) receive, aggregate, analyze, and secure reports that lead to the identification of tactics, techniques, and procedures used to perpetrate cyber incidents and ransomware attacks;

(2) RVISIBILITY.—The Council shall—
(A) receive, aggregate, analyze, and secure reports that lead to the identification of tactics, techniques, and procedures used to perpetrate cyber incidents and ransomware attacks;

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

(C) receive, aggregate, analyze, and secure reports that lead to the identification of tactics, techniques, and procedures used to perpetrate cyber incidents and ransomware attacks;
"(9) publish quarterly unclassified, public reports that may be based on the unclassified information contained in the briefings required under subsection (c);"

"(10) effectively identify opportunities, consistent with the protections in section 2235, to leverage and utilize data on ransomware attacks to support operations to track, and seize ransom payments utilizing virtual currencies, to the greatest extent practicable;"

"(12) on a not less frequently than annual basis, analyze public disclosures made pursuant to parts 229 and 219 of title 17, Code of Federal Regulations, or any subsequent document submitted to the Securities and Exchange Commission by entities experiencing cyber incidents and compare such disclosures to reports received by the Center; and"

"(13) in accordance with section 2235 and subsection (b) of this section, as soon as possible but not later than 24 hours after receiving a covered cyber incident report, ransom payments similarly submitted information pursuant to section 2235, or information received pursuant to a request for information or subpoena under section 2254, make available to the Director and the Director of the Office of Management and Budget—"

"(1) may establish a specific time requirement for sharing information under subsection (a)(13); and"

"(2) shall determine the appropriate Federal agencies under subsection (a)(13)."

"(c) PERIODIC BRIEFING.—Not later than 60 days after the effective date of the final rule required under section 2232 and on the first day of each month thereafter, the Director, in consultation with the National Cyber Director, the Attorney General, and the Director of National Intelligence, shall provide to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a briefing that characterizes the national cyber threat landscape, including the threat facing Federal agencies and covered entities, and applicable intelligence and law enforcement information, covered cyber incidents, and ransomware attacks, as of the date of the briefing, which shall include—"

"(1) include the total number of reports submitted under sections 2232 and 2233 during the preceding month, including a breakdown of known used vulnerabilities, ransomware attacks, and cyber incident or a ransom payment occurs following an exempted threat described in paragraph (6), and otherwise perform analyses, consistent with the protections in section 2235, to leverage and utilize data on ransomware attacks to support operations to track, and seize ransom payments utilizing virtual currencies, to the greatest extent practicable;"

"(2) in a substantially similar timeframe, which shall include a summary of the known uses of the information in reports submitted under sections 2232 and 2233 and be unclassified, but may include a classified annex.

"SEC. 2232. REQUIRED REPORTING OF CERTAIN CYBER INCIDENTS.

"(a) In General.—"

"(1) COVERED CYBER INCIDENT REPORTS.—A covered entity that is a victim of a covered cyber incident shall report the covered cyber incident to the Director not later than 24 hours after the covered entity reasonably believes that the covered cyber incident has occurred.

"(2) RANSOM PAYMENT REPORTS.—A covered entity, except for an individual or a small organization, that makes a ransom payment as a result of a ransomware attack against the covered entity or a ransom payment to the Director not later than 24 hours after the ransom payment has been made.

"(3) SUPPLEMENTAL REPORTS.—A covered entity shall promptly submit to the Director an update or supplement to a previously submitted covered cyber incident report if new or different information becomes available or if the covered entity makes a ransom payment after submitting a covered cyber incident report required under paragraph (1)."

"(C) PERIODIC BRIEFING.—Any covered entity subject to requirements of paragraph (1), (2), or (3) shall preserve data relevant to the covered cyber incident or ransom payment pursuant to procedures established in the final rule issued pursuant to subsection (b).

"(4) EXCEPTIONS.—"

"(A) REPORTING OF COVERED CYBER INCIDENT WITH RANSOM PAYMENT.—If a covered cyber incident includes a ransom payment such that the reporting requirements under paragraphs (1), (2), and (3) shall not apply to a covered entity required by law or regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe.

"(B) SUBSTANTIALLY SIMILAR REPORTED INFORMATION.—The requirements under paragraphs (1), (2), and (3) shall not apply to a covered entity required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe.

"(C) DOMAINS SYSTEMS.—The requirements under paragraphs (1), (2), and (3) shall not apply to an entity or the functions of an entity that is a domain name system, domain name system entity, or internet Assigned Numbers Authority.

"(D) MANAGEMENT, TIMING, AND FORM OF REPORTS.—Reports made under paragraphs (1), (2), and (3) shall be made in the manner and form, and within the time period in the case of reports made under paragraph (3), prescribed in the final rule issued pursuant to subsection (b).

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

"(C) DOMAINS SYSTEMS.—The requirements under paragraphs (1), (2), and (3) shall not apply to an entity or the functions of an entity that is a domain name system, domain name system entity, or internet Assigned Numbers Authority.

"(D) MANAGEMENT, TIMING, AND FORM OF REPORTS.—Reports made under paragraphs (1), (2), and (3) shall be made in the manner and form, and within the time period in the case of reports made under paragraph (3), prescribed in the final rule issued pursuant to subsection (b).

"(C) PERIODIC BRIEFING.—Not later than 2 years after the date of enactment of this section, the Director, in consultation with the Director of National Intelligence, the Secretaries of Treasury, Commerce, and Homeland Security, and the Director of the Office of Management and Budget, shall publish in the Federal Register a notice of proposed rulemaking to implement subsection (a).

"(D) EFFECTIVE DATE.—Paragraphs (1) and (2) shall take effect on the dates prescribed in the final rule issued pursuant to paragraph (1), the Director shall issue a final rule to implement subsection (a).

"(E) SUBSEQUENT RULEMAKINGS.—"

"(A) In General.—The Director is authorized to issue rules to amend or revise the final rule issued pursuant to paragraph (2).

"(B) PROCEDURES.—Any subsequent rules issued under paragraph (A) shall comply with the requirements under chapter 5 of title 5, United States Code, including the issuance of a notice of proposed rulemaking under section 553 of such title.

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

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

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

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

"(C) the extent to which damage, disruption, or unauthorized use of a covered entity, or the functions of such an entity, including the accessing of sensitive cybersecurity vulnerability information or the results of vulnerability testing services, will enable the disruption of the reliable operation of critical infrastructure.

"(2) A clear description of the types of subsectors that constitute covered entities, based on—"

"(A) the unauthorized access to an information system or network with a substantial loss of confidentiality, integrity, or availability, such as information systems or networks on which a serious impact on the safety and resiliency of operational systems and processes;"

"(B) a disruption of business or industrial operations due to a cyber incident; or"

"(C) an occurrence described in clause (i) or (ii) due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise; and"

"(D) the sophistication or novelty of the tactics used to disrupt such an event, as well as the type, volume, and sensitivity of the data at issue;"

"(E) the number of individuals directly or indirectly affected or potentially affected by such an incident; and"

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

"(G) exclude—"

"(i) any event where the cyber incident is perpetuated by good faith security research or a response to an invitation by the owner or operator of the information system for third parties to find vulnerabilities in the information system, such as through a vulnerability disclosure program or the use of authorized penetration testing services; and"

"(ii) the threat of disruption as extortion, as described in section 2201(i)(9).

"(2) REQUIRED COVERAGE.—The Director shall require that a covered cyber incident or a ransom payment occurs following an exempted threat described in paragraph (6), and otherwise perform analyses, consistent with the protections in section 2235, to leverage and utilize data on ransomware attacks to support operations to track, and seize ransom payments utilizing virtual currencies, to the greatest extent practicable; and"

"(7) IN GENERAL.—The Director, in consultation with the Secretary of the Treasury, the Secretary of Commerce, and the Secretary of Homeland Security, shall publish in the Federal Register a notice of proposed rulemaking to implement subsection (a).

"(8) FINAL RULE.—Not later than 2 years after publication of the notice of proposed rulemaking under paragraph (1), the Director shall issue a final rule to implement subsection (a)."
and available, with respect to a covered cyber incident:

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

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

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

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

(iv) the impact to the operations of the covered entity;

(B) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetuate the covered cyber incident;

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

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

(E) The name and other information that clearly identifies the entity impacted by the covered cyber incident.

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

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

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

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

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

(D) Any additional information that clearly identifies the entity that made the ransom payment.

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

(F) The date of the ransom payment.

(G) The ransom payment demand, including the type of virtual currency or other commutable form of payment, if applicable.

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

(I) The amount of the ransom payment.

(J) A clear description of the types of data required under paragraph (1) and the period of time for which the data is required to be preserved.

“(H) The ransom payment instructions, in- cluding where applicable, the service provider of such entity to assist with compliance with the reporting requirements of a covered cyber incident.

(i) a description of the unauthorized access where applicable, the service provider of such entity to assist with compliance with the reporting requirements of a covered cyber incident.

(ii) a description of the unauthorized access where applicable, the service provider of such entity to assist with compliance with the reporting requirements of a covered cyber incident.

(iii) the estimated date range of such incident;

(iv) the impact to the operations of the covered entity;

(C) The name and other information that clearly identifies the entity impacted by the covered cyber incident.

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

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

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

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

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

(D) Any additional information that clearly identifies the entity that made the ransom payment.

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

(F) The date of the ransom payment.

(G) The ransom payment demand, including the type of virtual currency or other commutable form of payment, if applicable.

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

(I) The amount of the ransom payment.

(J) A clear description of the types of data required under paragraph (1) and the period of time for which the data is required to be preserved.

“(7) Deadlines for submitting reports to the Director required under subsection (a)(3), which shall—

(A) be established by the Director in consultation with the NCA; and

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

(C) balance the need for situational awareness with the ability of the covered entity to conduct incident response and inves- tigations.

“(8) Procedures for—

(A) entities to submit reports required by paragraphs (1) and (2) of subsection (a), including the manner and form thereof, which shall include, at a minimum, a concise, user-friendly web-based form;

(B) the means by which the Center to carry out the enforce- ment provisions of section 2233, including with respect to the issuance, service, withdrawal, and enforcement of subpoenas, appeals and due process procedures, the suspension and debarment provisions in section 2234(c), and other aspects of noncompliance;

(C) implementing the exceptions provided in subsection (a)(3) and (a)(4) and the period of time for which the data is required to be preserved.

“(9) A clear description of the types of en- tities that constitute other private sector entities for purposes of section 2228(h)(7).

“(10) Third Party Report Submission and Ransom Payment.—

(T) First Submission.—An entity, including a covered entity, that is required to submit a covered cyber incident report or a ransom payment report may use a third party, such as an incident response company, insurance provider, information sharing and analysis organization or law firm, to submit the required report under subsection (b)(1).

“(11) Ransom Payment.—If an entity impacted by a ransomware attack uses a third party to make a ransom payment, the third party shall not be required to submit a ransom payment report for itself under subsection (a)(2).

“(12) Duty to Report.—Third-party report- ing under paragraph (10) does not relieve a covered entity or an entity that makes a ransom payment from the duty to comply with the requirements for covered cyber inci- dent reports or ransom payment reports.

“(13) Responsibility to Advise.—Any third party used by an entity that knowingly makes a ransom payment on behalf of an entity impacted by a ransomware attack shall advise the impacted entity of the responsibilities of the impacted entity regarding reporting ransom payments under this section.

“(14) Outreach to Covered Entities.—

(A) In General.—The Director shall con- duct, and the Director may request other entities to participate in, an outreach and education campaign to cover- ed cyber incident reports and ransom payment reports that is known to be personal information of a specific individual or infor- mation that identifies a specific individual that is not directly related to a cybersecurity threat.

(B) The outreach and education campaign under paragraph (1) shall—

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

(ii) a description of the Center’s events and programs; and

(iii) sector coordinating councils; and

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

“(15) Organization of Reports.—Notwith- standing section 35 of title 44, United States Code, commonly known as the ‘Paperwork Reduction Act’, the Director may request information within the scope of the final rule issued under subsection (b) by the alter- nation of existing questions or response fields and the reorganization and reformattting of the means by which covered cyber incident reports, ransom payment reports, and any voluntarily offered information is submitted to the Center.

“SEC. 2233. VOLUNTARY REPORTING OF OTHER CYBER INCIDENCE.

“(a) In General.—Entities may voluntarily report incidents or ransom payments to the Director that are not required under paragraph (1), (2), or (3) of section 2223(a), but may enhance the situational awareness of cyber threats.

“(b) Voluntary Provision of Additional Information in Required Reports.—Enti- ties may voluntarily include in reports required under paragraph (1), (2), or (3) of section 2232(a) information that is not required to be included, but may enhance the situational awareness of cyber threats.

“(c) Application of Protections.—The protections under section 2233 applicable to covered cyber incident reports shall apply in the same manner and to the same extent to reports and information submitted under subsections (a) and (b).

“SEC. 2234. NONCOMPLIANCE WITH REQUIRED REPORTING.

“(a) Purpose.—In the event that an entity that is required to submit a report under section 2233(a) fails to comply with the require- ments of paragraphs (1), (2), and (3) of subsection (a), the Director may—

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

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

(C) An overview of the protections afforded to covered entities for complying with the requirements under paragraphs (1), (2), and (3) of subsection (a).

(D) An overview of the steps taken under section 2234 when a covered entity is not in compliance with the reporting requirements under subsection (a).

(E) Specific outreach to cybersecurity vendors, incident response providers, cyber- security insurance entities, and other enti- ties that may support covered entities or ransomware attack victims.

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

(G) Coordination.—In conducting the out- reach and education campaign required under paragraph (1), the Director may coordinate with—

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

(B) industry associations; and

(C) information sharing and analysis cen- ters.

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

“(f) Organization of Reports.—Notwith- standing section 35 of title 44, United States Code, commonly known as the ‘Paperwork Reduction Act’, the Director may request information within the scope of the final rule issued under subsection (b) by the alteration of existing questions or response fields and the reorganization and reformattting of the means by which covered cyber incident reports, ransom payment reports, and any voluntarily offered information is submitted to the Center.
pursuant to subsection (c), to gather information sufficient to determine whether a covered cyber incident or ransom payment has occurred, and, if so, whether additional action is warranted pursuant to subsection (d).

"(b) INITIAL REQUEST FOR INFORMATION.—

"(1) IN GENERAL.—If the Director has reason to believe, through analysis performed pursuant to paragraph (1) or (2) of section 2232(a), that an entity has experienced a covered cyber incident or ransom payment, the Director may issue a subpoena pursuant to subsection (c), that the facts relating to the covered cyber incident or ransom payment at issue may constitute grounds for a regulatory enforcement action or criminal prosecution, the Attorney General or the appropriate Federal regulatory agency may use that information for a regulatory enforcement action or criminal prosecution.

"(2) APPLICATION TO CERTAIN ENTITIES AND OTHERS.—If an initial request pursuant to paragraph (1) or a covered cyber incident or ransom payment report submitted to the Center by an entity that makes a ransom payment or third party under section 2232 shall not be used by any Federal, State, Tribal, or local government to investigate or take another law enforcement action against the entity that makes a ransom payment or third party.

"(3) RULE OF CONSTRUCTION.—Nothing in this subtitle shall be construed to provide an entity that submits a covered cyber incident or ransom payment report under section 2232 any immunity from law enforcement action for making a ransom payment otherwise prohibited by law.

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

"(1) the size and complexity of the entity;
"(2) the complexity in determining if a covered cyber incident has occurred; and
"(3) prior interaction with the Agency or awareness of the entity of the policies and procedures of the Agency for reporting covered cyber incidents and ransom payments.

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

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

"(1) issued an initial request for information pursuant to subsection (b);
"(2) issued a subpoena pursuant to subsection (c) or (d); or
"(3) referred a matter to the Attorney General for a civil action pursuant to subsection (c)(2).

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

"(1) issued an initial request for information pursuant to subsection (b); or
"(2) issued a subpoena pursuant to subsection (c).

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

SEC. 2315. INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.

(a) DISCLOSURE, RETENTION, AND USE.—Information provided to the Center or Agency pursuant to section 2232 or 2233 may be disclosed to, retained by, and used by, consistent with otherwise applicable law, any Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

"(A) a cybersecurity purpose;
"(B) VENUE.—An action under this paragraph may be brought in a judicial district in which the activity against which the action is brought resides, is found, or does business.

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

("(D) DEPARTMENT OF FEDERAL CONTRACTORS.—The Director may require the subcontractor to comply with a subpoena issued under this subsection—

"(a) the entity that makes a ransom payment or third party under section 2232 shall be retained, used, and disseminated, where permissible and appropriate, by the Federal Government in accordance with any processes adopted pursuant to section 105 of the Cybersecurity Act of 2015 (6 U.S.C. 1503) and any information contained in those reports, are collected, stored, and protected at a minimum in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication 199, or any successor document.

"(5) PROHIBITION ON USE OF INFORMATION ABOUT A COVERED CYBER INCIDENT OR RANSOM PAYMENT OBTAINED SOLELY THROUGH RECEIVING A SUBPOENA DURING A CYBER THREAT INDICATORS AND DEBAR.—

"(6) NO WAIVER OF PRIVILEGE OR PROTECTION.—The submission of a report to the Center or Agency pursuant to section 2232 shall not constitute a waiver of any applicable privilege or protection, including trade secret protection and attorney-client privilege.
"(c) EXEMPTION FROM DISCLOSURE.—Information contained in a report submitted to the Office under section 2322 shall be exempt from disclosure under section 552(b)(3)(B) of title 5, United States Code (commonly known as the "Freedom of Information Act") and any State, Tribal, or local provision of law requiring disclosure of information or record contained in such report.

"(d) EX PARTE COMMUNICATIONS.—The submission of a report to the Agency under section 2322 shall not be subject to a rule of any Federal department or agency or any judicial doctrine regarding ex parte communications with a decision-making official.

"(e) LIMITATION ON PROCEDURES.—No proceeding, action, or proceeding described in subparagraph (A) shall apply to records created in the course of preparing, drafting, or submitting such report.

"(f) S HARING WITH NON-FEDERAL ENTITIES.—The Agency shall anonymize the victim who reported the information when making information provided in reports received pursuant to this section available to suitable recipients, including entities that make a ransom payment report to the Center for the purpose of preparing, drafting, or submitting such report, may be received in evidence, subject to discovery, or otherwise used in any material, hearsay or other proceeding in or before any court, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, unless the information is included in a report that creates or requires the participant to create a defense to discovery or otherwise affect the discovery of any communication, document, material, or other record not created for the sole purpose of preparing, drafting, or submitting such report.

"(g) PROPRIETARY INFORMATION.—Information contained in a report submitted to the Agency under section 2322 shall be exempt from disclosure under section 552(b)(3)(B) of title 5, United States Code (commonly known as the "Freedom of Information Act") and any State, Tribal, or local provision of law requiring disclosure of information or record contained in such report.

"(h) STORED COMMUNICATIONS ACT.—Nothing in this subtitle shall be construed to permit or require disclosure by a provider of an electronic communication service to the public of information not otherwise permitted or required to be disclosed under chapter 11 of title 18, United States Code (commonly known as the 'Stored Communications Act').

"(i) UNITED STATES AND CONFORMING AMENDMENT.—The table of contents in section 1(b) of this title shall be amended to include a reference to this subtitle.

"(j) CYBER INCIDENT REPORTING SHARING.—Sec. 2323. Information shared with or provided by the Federal Government.

"(k) FEDERAL SHARING OF INCIDENT REPORT SHARING.—Sec. 2324. Voluntary reporting of certain cyber incidents.

"(l) NONCOMPLIANCE WITH REQUIRED REPORTING.—Sec. 2325. Noncompliance with required reporting.
with the Attorney General and the Director of the Federal Bureau of Investigation, shall establish and chair the Joint Ransomware Task Force to coordinate an ongoing nationwide campaign against ransomware attacks, and identify and pursue opportunities for international cooperation.

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

(3) RESPONSIBILITIES.—The Joint Ransomware Task Force, utilizing only existing authorities of each participating agency, shall:

(A) prioritize the Federal agencies and non-Federal entities, including the private sector, to improve Federal actions against ransomware threats;

(B) facilitating coordination and collaboration between Federal entities and relevant entities, including the private sector, to improve Federal actions against ransomware threats;

(C) collection, sharing, and analysis of ransomware trends to inform Federal actions;

(D) creation of after-action reports and other lessons learned from Federal actions that identify successes and failures to improve subsequent actions;

(H) any other activities determined appropriate by the task force to mitigate the threat of ransomware attacks against Federal agencies and entities.

(b) REPORT ON OPPORTUNITIES TO STRENGTHEN SECURITY RESEARCH.—Not later than 1 year after the date of enactment of this Act, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report describing how the National Cybersecurity and Communications Integration Center, established under section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 6103) has carried out activities under section 2231(a)(9) of the Homeland Security Act of 2002, as added by section 6103(a) of this Act, by proactively identifying pressing cyber threat data to inform and enable cybersecurity research within the academic and private sector.

(c) REPORT ON RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM.—Not later than 1 year after the date of enactment of this Act and annually thereafter for the duration of the pilot program established under section 6105, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report that includes:

(1) the effectiveness of the notifications under section 6105(c) in mitigating security vulnerabilities and the threat of ransomware;

(2) identification of the most common vulnerabilities utilized in ransomware;

(3) the number of notifications issued during the preceding year;

(4) to the extent practicable, the number of vulnerable devices or systems mitigated under this pilot by the Agency during the preceding year;

(d) REPORT ON HARMONIZATION OF REPORTING REQUIREMENTS.—(1) IN GENERAL.—Not later than 180 days after the date on which the National Cyber Director convenes the council described in section 1752(c)(1)(H), the National Cyber Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives a report that includes:

(A) a list of duplicative Federal cyber incident reporting requirements on covered entities and entities that make a ransom payment; and

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

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

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

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

(e) GAO REPORTS.—

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

(2) EXEMPTIONS TO REPORTING.—Not later than 1 year after the date on which the Director issues the final rule required under section 6103(a) of this title, the Comptroller General of the United States shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the implementation of this Act and the amendments made by this Act.

(f) REPORT ON EFFECTIVENESS OF ENFORCEMENT MECHANISMS.—Not later than 1 year after the date on which the Director issues the final rule required under section 6103(a) of the Homeland Security Act of 2002, as added by section 6103 of this title, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the effectiveness of the enforcement mechanisms within section 2224 of the Homeland Security Act of 2002, as added by section 6103 of this title.

TITLE LXII—CISA TECHNICAL CORRECTIONS AND IMPROVEMENTS ACT OF 2021

SEC. 6202. REDESIGNATIONS.

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

(1) by redesignating section 2217 (6 U.S.C. 665c) as section 2218; and

(2) by redesigning section 2216 (6 U.S.C. 665e) as section 2219;

(b) TECHNICAL AND CONFORMING AMENDMENTS.—Section 2220 of the Homeland Security Act of 2002 (6 U.S.C. 665b) is redesignated as section 2215.

(1) by striking “‘Homeland Security Act’ and inserting ‘‘Homeland Security Act of 2002’’.

(2) by redesigning section 2217 (6 U.S.C. 665c) as section 2218;

(3) by redesigning the fourth section 2215 (relating to the Director) as section 2216 (relating to the Director); and

(4) by redesigning the second section 2215 (relating to the Joint Cyber Planning Office) as section 2217 (relating to the Joint Cyber Planning Office).

(6) (a) [amended] by redesigning section 2216 (relating to the Director) as section 2217 (relating to the Director).

(b) TECHNICAL AND CONFORMING AMENDMENTS.—Section 2202(c) of the Homeland Security Act of 2002 (6 U.S.C. 652(c)) is amended—

(1) in paragraph (11), by striking “and” at the end;

(2) in the first paragraph (12)—

(A) by striking “section 2215” and inserting “section 2217”;

(B) by striking “and” at the end; and

(3) by redesigning the second and third paragraphs (12) as paragraphs (13) and (14), respectively.

(c) ADDITIONAL TECHNICAL AMENDMENT.—


(2) EFFECTIVE DATE.—The amendment made by paragraph (1) shall take effect as if
enacted as part of the DOTGOV Act of 2020
(title IX of division U of Public Law 116–269).
SEC. 6203. CONSOLIDATION OF DEFINITIONS.
(a) In General.—Title XXII of the Homeland
Security Act of 2002 (42 U.S.C. 6501 et seq.) is amended by inserting before the subtitle A following the heading the following:
SEC. 6200. DEFINITIONS.
(1) Agency.—The term ‘Agency’ means the Cybersecurity and Infrastructure Security Agency.
(2) Agency information.—The term ‘agency information’ means information collected or maintained by or on behalf of an agency.
(3) Agency information system.—The term ‘agency information system’ means an information system used or operated by an agency or by another entity on behalf of an agency.
(4) Appropriate congressional committees.—The term ‘appropriate congressional committees’ 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.
(5) Cloud service provider.—The term ‘cloud service provider’ means an entity offering products or services related to cloud computing as defined by the National Institutes of Standards and Technology in NIST Special Publication 800–145 and any amending or superseding document relating thereto.
(6) Critical infrastructure information.—The term ‘critical infrastructure information’ means information not customarily in the public domain and related to the security of critical infrastructure or protected systems, including—
(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;
(B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation;
(C) any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation, thereto, risk management planning, or risk audit; or
(D) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.
(7) Cyber threat indicator.—The term ‘cyber threat indicator’ means information that is necessary to describe or identify—
(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or a protected system, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, so as to ensure the availability, integrity, and reliability thereof;
(B) communicating or disclosing critical infrastructure information, including cybersecurity risks and incidents, to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B); or
(C) voluntarily disseminating critical infrastructure information, including cybersecurity risks and incidents, to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).
(8) Cybersecurity purpose.—The term ‘cybersecurity purpose’ means the purpose of protecting an information system or information systems, including any planned or past assessment, projection, or estimate of the vulnerability of a cybersecurity threat or security vulnerability.
(9) Cybersecurity risk.—The term ‘cybersecurity risk’ means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism; and
(10) Cybersecurity threat.—
(A) In General.—Except as provided in subparagraph (B), the term ‘cybersecurity threat’ means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.
(B) Exclusion.—The term ‘cybersecurity threat’ does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.
(11) Defensive measure.—
(A) In General.—Except as provided in subparagraph (B), the term ‘defensive measure’ means an action, device, procedure, signature, technique, or other measure applied to a transaction, communication, or transaction system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.
(B) Exclusion.—The term ‘defensive measure’ does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by—
(i) the entity operating the measure; or
(ii) another legal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.
(12) Homeland Security Enterprise.—The term ‘Homeland Security Enterprise’ means relevant governmental and non-governmental entities involved in homeland security, including State, local, and Tribal government officials, private sector representatives, academics, and other policy experts.
(13) Incident.—The term ‘incident’ means an occurrence that actually or imminently jeopardizes, without lawful authority, an information system.
(14) Information sharing and analysis organization.—The term ‘Information Sharing and Analysis Organization’ means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of—
(A) gathering and analyzing critical infrastructure information, including information related to cybersecurity risks and incidents, in order to better understand security problems and interdependencies related to critical infrastructure, including cybersecurity risks and incidents, to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B); or
(B) communicating or disclosing critical infrastructure information, including cybersecurity risks and incidents, to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).
(15) Information system.—The term ‘information system’ has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).
(16) Intelligence community.—The term ‘intelligence community’ has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).
(17) Managed service provider.—The term ‘managed service provider’ means any entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer or a consumer, including any planned or past assessment, projection, or estimate of the vulnerability of a cybersecurity threat or security vulnerability.
(18) Malicious cyber command and control.—
(A) In General.—The term ‘malicious cyber command and control’ means an unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism; and
(B) Exclusion.—The term ‘malicious cyber command and control’ does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.
(19) Managed service provider.—The term ‘managed service provider’ means any entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer or a consumer, including any planned or past assessment, projection, or estimate of the vulnerability of a cybersecurity threat or security vulnerability.
(20) National security system.—The term ‘national security system’ has the meaning given the term in title 40, United States Code.
(21) Ransom payment.—The term ‘ransom payment’ means the transmission of any wired or wireless communication, including any planned or past assessment, projection, or estimate of the vulnerability of a security threat or security vulnerability.
“(A) means a cyber incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism, such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data, information, programs, processes, or data centers, to cause a sector to jeopardize the confidentiality, integrity, and availability of an information system or its information;

“(B) does not include any such event where the damage is made by a Federal Government entity, good faith security research, or in response to an invitation by the owner or operator of an information system for third parties to identify vulnerabilities in the information system.

“(23) SECTOR RISK MANAGEMENT AGENCY.—The term ‘Sector Risk Management Agency’ means a Federal department or agency, designated by law or Presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sectors and environment in coordination with the Department.

“(24) SECURITY CONTROL.—The term ‘security control’ means the management, operation, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

“(25) SECURITY VULNERABILITY.—The term ‘security vulnerability’ means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

“(26) SHARING.—The term ‘sharing’ (including ‘information sharing’ and ‘disseminating’ (including all conjugations of each such term).

“(27) SUPPLY CHAIN COMPROMISE.—The term ‘supply chain compromise’ means a disruption that occurs at any point during the life cycle of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical information system or the information the system processes, stores, or transmits, and can occur at any point during the life cycle.

“(28) SUPPLY CHAIN VULNERABILITY.—The term ‘supply chain vulnerability’ means the digital representation of value that functions as a medium of exchange, a unit of account, or a store of value.

“(29) VIRTUAL CURRENCY.—The term ‘virtual currency’ means any unique public cryptographic key identifying the location to which a virtual currency payment can be made.”.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

(1) by amending section 2201 and inserting the following:

“Sec. 2201. Definition.”;

(2) by striking paragraphs (3), (5), and (8); and

(3) by redesigning paragraphs (4) as paragraphs (3) and (4), respectively.

(4) by redesigning paragraphs (6) and (7) as paragraphs (4) and (5), respectively.

(5) in section 2209—

(A) by striking subsection (a); and

(B) by redesigning subsections (b) through (o) as subsections (a) through (n), respectively.

(6) in subsection (c)(1)—

(i) in subparagraph (A)(iii), as so redesignated, by striking “, as that term is defined under section 3003(4) of the National Security Act of 1947”;

(ii) in subparagraph (B), by striking “‘information sharing and analysis organizations’”;

(7) in subsection (d), as so redesignated—

(i) in the matter preceding paragraph (1), by striking “subsection (c)” and inserting “subsection (b)”; and

(ii) in paragraph (1)(E)(ii)(I), by striking “‘information sharing and analysis organizations’”;

(8) in subsection (e), as so redesignated, by striking “subsection (c)(8)” and inserting “subsection (b)(8)”; and

(9) in subsection (f), as so redesignated—

(i) in paragraph (1)(A), by striking “subsection (c)(12)” and inserting “subsection (b)(12)”; and

(ii) in paragraph (1)(B)(i), by striking “subsection (c)(12)” and inserting “subsection (b)(12)”; and

(10) in section 2210—

(A) by striking subsection (a); and

(B) by redesigning subsections (b) through (d) as subsections (a) through (c), respectively.

(11) in subsection (c), as so redesignated, by striking “subsection (c)” and inserting “subsection (b)”; and

(12) in section 2211, by striking subsection (h).

(13) in section 2212, by striking “information sharing and analysis organizations (as defined in section 2222(5))” and inserting “Information Sharing and Analysis Organizations”;

(14) in section 2213—

(A) by striking subsection (a); and

(B) by redesigning subsections (b) through (f) as subsections (a) through (e), respectively;

(15) in subsection (c), as so redesignated, by striking “subsection (c)” and inserting “subsection (b)”; and

(16) in subsection (d), as so redesignated, by striking “subsection (c)” and inserting “subsection (b)”; and

(17) in section 2216, as so redesignated—

(A) in subsection (d)(2), by striking “information sharing and analysis organizations” and inserting “Information Sharing and Analysis Organizations”;

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

“(f) CYBER DEFENSE OPERATION DEFINED.—In this section, the term ‘cyber defense operation’ means the use of a defensive measure.”;

“(1) in section 2218(c)(4)(A), as so redesignated, by striking “, as that term is defined under section 3003(4) of the National Security Act of 1947”;

“(2) in section 2219(c), as so redesignated, by striking “cyber defense operation’’; hazards environment.”.

“(28) SUPPLY CHAIN VULNERABILITY.—The term ‘supply chain vulnerability’ means the unique public cryptographic key identifying the location to which a virtual currency payment can be made.”

(c) TABLE OF CONTENTS AMENDMENTS.—The table of contents in section 102 of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended—

(1) by inserting below the item relating to title XXII the following:

“Sec. 2200. Definitions.”;

(2) by striking the item relating to section 2201 and inserting the following:

“Sec. 2201. Definitions.”;

(3) by striking the item relating to section 2211 and all that follows through the item relating to section 2217 and inserting the following:

“Sec. 2211. National Asset Database.

Sec. 2215. Duties and authorities relating to .gov internet domain.

Sec. 2216. Joint Cyber Planning Office.

Sec. 2217. Cybersecurity State Coordinator.

Sec. 2218. Sector Risk Management Agencies.

Sec. 2219. Cybersecurity Advisory Committee.

Sec. 2220. Cybersecurity Education and Training Programs.”.

(d) CYBERSECURITY ACT OF 2015 DEFINITIONS.—Section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501) is amended—

(1) by striking paragraphs (4) through (7) and inserting the following:

“(4) CYBERSECURITY PURPOSE.—The term ‘cybersecurity purpose’ has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

“(5) CYBERSECURITY THREAT.—The term ‘cybersecurity threat’ has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

“(6) CYBER THREAT INDICATOR.—The term ‘cyber threat indicator’ has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

“(7) DEFENSIVE MEASURE.—The term ‘defensive measure’ has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

“(8) MONITOR.—The term ‘monitor’ has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

“(9) SECURITY VULNERABILITY.—The term ‘security vulnerability’ has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

“SEC. 6204. ADDITIONAL TECHNICAL AND CONFORMING AMENDMENTS.

(a) FEDERAL CYBERSECURITY ENHANCEMENT ACT OF 2015.—The Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1521 et seq.) is amended—

(1) in section 2226 (6 U.S.C. 1521)—

(A) in paragraph (2), by striking “section 2226” and inserting “section 2209”; and

(B) in paragraph (4), by striking “section 2209” and inserting “section 2200”;
SEC. 6301. EXEMPTION FROM FEDERAL CYBERSECURITY REQUIREMENTS.

(a) In General.—Section 223(b)(2) of the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1523(b)(2)) is amended to read as follows:

"(A) in general.—A particular requirement under subparagraph (1) shall not apply to an agency information system of an agency if—

(i) with respect to the agency information system, the head of the agency submits to the Director an application for an exemption from the particular requirement, in which the head of the agency personally certifies to the Director with particularity that—

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

(II) the particular requirement is not necessary for the agency information system or agency information stored on or transiting the agency information system;

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

(iv) (B) by striking sections 2213(c)(2) and inserting "section 2213(c)(2)".


(c) Defense Institution.—The term "financial institution" means a financial institution specified in subparagraph (A), (B), (C), (D), (E), (F), (G), (H), (I), (J), (M), or (Y) of section 5312(a)(2) of title 31, United States Code.

(d) Foreign Personal.—The term "foreign personal" means an individual or entity that is not a United States person.

(e) Knowingly.—The term "knowingly" with respect to conduct, a circumstance, or a result, means that a person has actual knowledge, or should have known, of the conduct, the circumstance, or the result.

(f) Economic and Financial Sanctions, when used as part of a coordinated and comprehensive strategy, are a powerful tool to advance United States foreign policy and national security interests.

(g) Violation of the Ordinance of the Russian Federation in Ukraine is a threat to the democratic sovereignty of Ukraine, a valued and key partner of the United States.

(h) Sanctions relating to the actions of the Russian Federation, when used as part of a coordinated and comprehensive strategy, are a powerful tool to advance United States foreign policy and national security interests.
the Russian Federation engages in escalatory military or other offensive operations against Ukraine.

**SEC. 1295. IMPOSITION OF SANCTIONS WITH RESPECT TO FOREIGN FINANCIAL INSTITUTIONS.**

(a) **LIST REQUIRED.**—Not later than 30 days after making an affirmative determination under section 1293(1) and every 90 days thereafter, the President shall submit to the appropriate congressional committees a list of foreign persons that the President determines are or come within the possession or control of a United States person.

(b) **OFFICIALS SPECIFIED.**—The officials specified in this subsection are the following:

(1) The President of the Russian Federation.

(2) The Prime Minister of the Russian Federation.

(3) The Foreign Minister of the Russian Federation.


(9) The Commander in Chief of the Navy of the Russian Federation.

(10) The Commander of the Strategic Rocket Forces of the Russian Federation.


(12) The Commander of the Special Support Forces of the Russian Armed Forces.

(c) **ADDITIONAL OFFICIALS.**—

(1) **LIST REQUIRED.**—Not later than 30 days after making an affirmative determination under section 1293(1), and every 90 days thereafter, the President shall submit to the appropriate congressional committees a list of foreign persons that the President determines are—

(A) senior officials of any branch of the armed forces of the Russian Federation leading any of the operations described in section 1293(1); or

(B) senior officials of the Government of the Russian Federation, engaged in planning or implementing such operations.

(2) **IMPOSITION OF SANCTIONS.**—Upon the submission of each list required by paragraph (1), the President shall impose the sanctions described in subsection (d) with respect to each foreign person identified on the list.

(d) **SANCTIONS DESCRIBED.**—The sanctions to be imposed with respect to a foreign person under this section are the following:

(1) **PROPERTY BLOCKING.**—The President shall exercise all of the powers granted by the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) to the extent necessary to block and prohibit all transactions in property and interests in property of the foreign person if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

(2) **ALIENS INADMISSIBLE FOR VISAS, ADMISSION, OR PAROLE.**—An alien described in subsection (b) or (c) is—

(i) inadmissible to the United States;

(ii) ineligible to receive a visa or other documentation to enter the United States; and

(iii) otherwise ineligible to be admitted or paroled into the United States or to receive any other benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

(3) **CURRENT VISAS REVOKED.**—

(1) **IN GENERAL.**—The visa or other entry documentation of an alien shall be revoked, regardless of whether such alien's other entry documentation is or was issued.

(ii) IMMEDIATE EFFECT.—A revocation under clause (i) shall—

(I) take effect immediately; and

(II) automatically cancel any other valid visa or entry documentation that is in the alien’s possession.

(4) **SDN BLOCKING.**—The President shall impose the sanctions described in subsection (b) with respect to any foreign person if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

(5) **SDN BLOCKING OF STATE-OWNED ENTERPRISES.**—

(A) the Government of the Russian Federation is engaged in or knowingly supporting a significant escalation in hostilities or hostile action in or against Ukraine, compared to the level of hostilities or hostile action in or against Ukraine prior to November 1, 2021; and

(B) if so, whether such escalation has the aim of undermining, overthrowing, or dismantling the Government of Ukraine, occupying the territory of Ukraine, or interfering with the sovereignty or territorial integrity of Ukraine; and

(2) submit to the appropriate congressional committees a report on that determination.

**SEC. 1296. PROHIBITION ON AND IMPOSITION OF SANCTIONS ON TRANSACTIONS INVOLVING RUSSIAN SOVEREIGN DEBT.**

(a) **PROHIBITION ON TRANSACTIONS.**—Upon making an affirmative determination under section 1293(1) and not later than 30 days following such a determination, the President shall prohibit all transactions by United States persons involving the sovereign debt of the Government of the Russian Federation issued on or after the date of the enactment of this Act, including governmental bonds.

(b) **IMPOSITION OF SANCTIONS WITH RESPECT TO STATE-OWNED ENTERPRISES.**—

(1) **IN GENERAL.**—Not later than 60 days after making an affirmative determination under section 1293(1), the President shall identify and impose the sanctions described in subsection (d) with respect to foreign persons that the President determines engage in transactions involving the debt—

(A) of not less than 10 entities owned or controlled by the Government of the Russian Federation; and

(B) that is not subject to any other sanctions imposed by the United States.

(2) **APPLICABILITY.**—Sanctions imposed under paragraph (1) shall apply with respect to debt of an entity described in subparagraph (A) of that paragraph that is issued after the date that is 90 days after the President makes an affirmative determination under section 1293(1).

(c) **LIST: IMPOSITION OF SANCTIONS.**—Not later than 30 days after making an affirmative determination under section 1293(1), and every 90 days thereafter, the President shall—

(1) submit to the appropriate congressional committees a list of foreign persons that the President determines are or come within the possession or control of a United States person.

(2) **ALIENS INADMISSIBLE FOR VISAS, ADMISSION, OR PAROLE.**—

(A) **VISAS, ADMISSION, OR PAROLE.**—An alien described in subsection (b) or (c) is—

(i) inadmissible to the United States;

(ii) ineligible to receive a visa or other documentation that is in the alien’s possession.

(ii) IMMEDIATE EFFECT.—A revocation under clause (i) shall—

(I) take effect immediately; and

(II) automatically cancel any other valid visa or entry documentation that is in the alien’s possession.

(3) **SDN BLOCKING.**—The President shall impose the sanctions described in subsection (b) with respect to any foreign person if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

(4) **SDN BLOCKING OF STATE-OWNED ENTERPRISES.**—

(A) the Government of the Russian Federation is engaged in or knowingly supporting a significant escalation in hostilities or hostile action in or against Ukraine, compared to the level of hostilities or hostile action in or against Ukraine prior to November 1, 2021; and

(B) if so, whether such escalation has the aim of undermining, overthrowing, or dismantling the Government of Ukraine, occupying the territory of Ukraine, or interfering with the sovereignty or territorial integrity of Ukraine; and

(2) submit to the appropriate congressional committees a report on that determination.

**SEC. 1297. IMPOSITION OF SANCTIONS WITH RESPECT TO NORD STREAM 2.**

(a) **IN GENERAL.**—Upon making an affirmative determination under section 1293(1) and not later than 30 days following such a determination, the President shall prohibit all transactions by United States persons involving the sovereign debt of the Government of the Russian Federation issued on or after the date of the enactment of this Act, including governmental bonds.
not later than 30 days following such a determination, the President shall impose the sanctions described in subsection (b) with respect to a foreign person that is—

(1) an individual identified for or responsible for the planning, construction, or operation of the Nord Stream 2 pipeline or a successor entity; and

(2) an individual identified for or responsible for the planning, construction, or operation of the South Stream pipeline or a successor entity.

SEC. 1299A. USE OF DEPARTMENT OF DEFENSE ACQUISITION FUND TO SUPPLY WEAPONS AND DEFENSE SERVICES OF UKRAINE.

(a) USE OF SPECIAL DEFENSE ACQUISITION FUND.—The Secretary of Defense, in accordance with the Secretary of State, shall utilize, to the maximum extent possible, the Special Defense Acquisition Fund established under section 2311 of title 10, United States Code, to acquire defense articles and defense services for the purpose of assisting and supporting the Armed Forces of Ukraine.

(b) USE OF LEASE AUTHORITY AND SPECIAL DEFENSE LEASE AUTHORITY AND SPECIAL DEFENSE LEASE AUTHORITY AND SPECIAL DEFENSE ACQUISITION FUND TO SUPPLY WEAPONS AND DEFENSE SERVICES OF UKRAINE.

SEC. 1299B. IMPLEMENTATION; REGULATIONS; PENALTIES.

(a) IMPLEMENTATION.—The President may exercise all authorities provided to the President under sections 235 and 236 of the International Emergency Economic Powers Act (50 U.S.C. 1702 and 1704) to carry out this subtitle.

(b) REGULATIONS.—The President shall issue such regulations, licenses, and orders as are necessary to carry out this subtitle.

(c) PENALTIES.—A violation of this subtitle shall be punishable by fine, imprisonment, or both. The President shall impose a penalty upon a person, and upon each officer and employee of a foreign or domestic entity, that violates this subtitle.

Sec. 1299C. EXCEPTIONS; WAIVER.

(a) EXCEPTIONS.—

(1) IN GENERAL.—The President may exercise all authorities provided to the President under sections 235 and 236 of the International Emergency Economic Powers Act (50 U.S.C. 1702 and 1704) to carry out this subtitle.

(b) PENALTIES.—A violation of this subtitle shall be punishable by fine, imprisonment, or both. The President may impose a penalty upon a person, and upon each officer and employee of a foreign or domestic entity, that violates this subtitle.

(c) PENALTIES.—A violation of this subtitle shall be punishable by fine, imprisonment, or both. The President may impose a penalty upon a person, and upon each officer and employee of a foreign or domestic entity, that violates this subtitle.

Sec. 1299D. TERMINATION.

This subtitle terminates on the date that is 3 years after the date of the enactment of this Act.

SA 4833. Mr. BARRASSO (for himself, Mr. CRUZ, and Mr. JOHNSON) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 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; and so voted:

At the end of subtitle D title XII add the following:

Sec. 1237. IMPOSITION OF SANCTIONS WITH RESPECT TO NORD STREAM 2.

(a) IN GENERAL.—Not later than 15 days after the date of the enactment of this Act, the President shall—

(1) impose sanctions under subsection (b) with respect to a foreign person that is—

(A) Nord Stream 2 AG or a successor entity;
(B) Matthias Warnig; and
(C) any other corporate officer of or principal shareholder with a controlling interest in Nord Stream 2 AG or a successor entity.

(2) impose sanctions under subsection (c) with respect to—
(A) Nord Stream 2 AG or a successor entity; and
(B) Matthias Warnig.

(b) INELIGIBILITY FOR VISAS, ADMISSION, OR PAROLE OF IDENTIFIED PERSONS AND CORPORATE OFFICERS.—
(1) IN GENERAL.—
(A) Visa, admission, or parole.—An alien described in subsection (a)(1)—
(i) ineligible to enter the United States;
(ii) ineligible to receive a visa or other documentation to enter the United States; and
(iii) otherwise ineligible to be admitted or paroled into the United States or to receive any other benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).
(B) Current visas revoked.—
(i) In general.—The visa or other entry documentation of an alien described in subsection (a)(1) shall be revoked, regardless of when such visa or other entry documentation was issued.
(ii) Immediate effect.—A revocation under clause (i) shall—
(I) take effect immediately; and
(II) automatically cancel any other valid visa or entry documentation that is in the alien’s possession.

(c) BLOCKING OF PROPERTY OF IDENTIFIED PERSONS.—The President shall exercise all powers granted to the President by the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) to the extent necessary to prohibit all transactions in all property and interests in property of a person described in subsection (a)(2) if such property and interests in property are in the United States or are or come within the possession or control of a United States person.

(d) IMPLEMENTATION; PENALTIES.—
(1) Implementation.—The President may exercise all authorities provided to the President under sections 203 and 205 of the International Emergency Economic Powers Act (50 U.S.C. 1702 and 1704) to carry out this section.

(2) Penalties.—A person that violates, attempts to violate, conspires to violate, or causes violation of this section or any regulation, license, or order issued to carry out this section shall be subject to the penalties set forth in subsections (b) and (c) of section 206 of the International Economic Sanctions Act (50 U.S.C. 1705) to the same extent as a person that commits an unlawful act described in subsection (a) of that section.

(e) EXCEPTIONS.—
(1) Exception for intelligence, law enforcement, and national security activities.—This section shall not apply to any authorized intelligence, law enforcement, or national security activities of the United States.

(2) Exception to comply with United Nations Headquarters Agreement.—Sanctions under this section shall not apply with respect to the admission of an alien to the United States if the admission of the alien is necessary to permit the United States to comply with the Agreement regarding the Headquarters of the United Nations, signed at Lake Success June 26, 1947, and entered into force November 21, 1947, between the United Nations and the United States, the Convention on Consular Relations, done at Vienna June 29, 1963, and entered into force March 19, 1967, or other applicable international obligations.

(3) Exception relating to importation of goods.—
(A) In general.—Notwithstanding any other provision of this section, the authority to impose sanctions under this section shall not include the authority or a requirement to impose sanctions on the importation of goods.

(B) Good definition.—In this paragraph, the term “good” means any article, natural or man-made substance, material, supply or manufactured product, including inspection and test equipment, and excluding technical data.

(f) SUNSET.—The authority to impose sanctions under this section shall terminate on the date that is 5 years after the date of the enactment of this Act.

(g) Definitions.—In this section:
(1) ADMISSION; ADMITTED; ALIEN.—The terms “admission”, “admitted”, and “alien” have the meanings given those terms in section 101 of the Immigration and Nationality Act (8 U.S.C. 1101).
(2) UNITED STATES PERSON.—The term “United States person” means—
(A) a United States citizen or an alien lawfully admitted for permanent residence to the United States;
(B) an entity organized or chartered in the United States; or
(C) any person within the United States.

AUTHORITY FOR COMMITTEES TO MEET

Mr. TESTER. Mr. President, I have 6 requests for committees to meet during today’s session of the Senate. They have the approval of the Majority and Minority Leaders.

Pursuant to rule XXVI, paragraph 5(a), of the Standing Rules of the Senate, the following committees are authorized to meet during today’s session of the Senate:

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

The Committee on Banking, Housing, and Urban Affairs is authorized to meet during the session of the Senate on Thursday, November 18, 2021, at 9:30 a.m., to conduct a hearing on a nomination.

COMMITTEE ON ENERGY AND NATURAL RESOURCES

The Committee on Energy and Natural Resources is authorized to meet during the session of the Senate on Thursday, November 18, 2021, at 10:15 a.m., to conduct a business meeting.

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

The Committee on Homeland Security and Governmental Affairs is authorized to meet during the session of the Senate on Thursday, November 18, 2021, at 10:15 a.m., to conduct a hearing on nominations.

COMMITTEE ON THE JDUDICIARY

The Committee on the Judiciary is authorized to meet during the session of the Senate on Thursday, November 18, 2021, at 9 a.m., to conduct a hearing.

SPECIAL COMMITTEE ON AGING

The Special Committee on Aging is authorized to meet during the session of the Senate on Thursday, November 18, 2021, at 9:30 a.m., to conduct a hearing.

PRIVILEGES OF THE FLOOR

Mr. REED. Mr. President, I ask unanimous consent that Leslie Ashton and Cami Pease, Government Accountability Office detailees to the Senate Armed Services Committee, have floor privileges during consideration of the fiscal year 2022 National Defense Authorization Act.

The PRESIDING OFFICER. Without objection, it is so ordered.

The PRESIDING OFFICER. The majority leader.

EXECUTIVE SESSION

EXECUTIVE CALENDAR

Mr. SCHUMER. Madam President, I ask unanimous consent that the Senate proceed to executive session to consider the following nominations en bloc: Calendar Nos. 332 and 444: that the Senate vote on the nominations en bloc without intervening action or debate; that the motions to reconsider be considered made and laid upon the table with no intervening action or debate; that any statements related to the nominations be printed in the RECORD; that the President be immediately notified of the Senate’s action, and the Senate resume legislative session.

There being no objection, the Senate proceeded to consider the nominations.

The PRESIDING OFFICER. The question is, Will the Senate advise and consent to the nominations of Lee Satterfield, of South Carolina, to be an Assistant Secretary of State (Educational and Cultural Affairs) and Jeffrey M. Hovenier, of Washington, a Career Member of the Senior Foreign Service, Class of Minister-Counselor, to be Ambassador Extraordinary and Plenipotentiary of the United States of America to the Republic of Kosovo en bloc?

The nominations were confirmed en bloc.

LEGISLATIVE SESSION

The PRESIDING OFFICER. The Senate will now resume legislative session.

ORDERS FOR FRIDAY, NOVEMBER 19, 2021

Mr. SCHUMER. Madam President, I ask unanimous consent that when the