AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

117TH CONGRESS
1ST SESSION

S. 2491

To amend the Homeland Security Act of 2002 to establish the National Cyber Resilience Assistance Fund, to improve the ability of the Federal Government to assist in enhancing critical infrastructure cyber resilience, to improve security in the national cyber ecosystem, to address Systemically Important Critical Infrastructure, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JULY 27, 2021

Mr. KING (for himself, Mr. ROUNDS, and Mr. SASSE) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

---

A BILL

To amend the Homeland Security Act of 2002 to establish the National Cyber Resilience Assistance Fund, to improve the ability of the Federal Government to assist in enhancing critical infrastructure cyber resilience, to improve security in the national cyber ecosystem, to address Systemically Important Critical Infrastructure, and for other purposes.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Defense of United States Infrastructure Act of 2021''.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

TITLE I—INVESTING IN CYBER RESILIENCY IN CRITICAL INFRASTRUCTURE

SEC. 101. ESTABLISHMENT OF THE NATIONAL CYBER RESILIENCE ASSISTANCE FUND.

(a) SENSE OF CONGRESS.—It is the sense of Congress that—

(1) the United States now operates in a cyber landscape that requires a level of data security, resilience, and trustworthiness that neither the United States Government nor the private sector alone is currently equipped to provide;

(2) the United States must deny benefits to adversaries who have long exploited cyberspace to their advantage, to the disadvantage of the United States, and at little cost to themselves;

(3) this new approach requires securing critical networks in collaboration with the private sector to promote national resilience and increase the security of the cyber ecosystem;

(4) reducing the vulnerabilities adversaries can target denies them opportunities to attack the interests of the United States through cyberspace;

(5) the public and private sectors struggle to coordinate cyber defenses, leaving gaps that decrease national resilience and create systemic risk;

(6) new technology continues to emerge that further compounds these challenges;

(7) while the Homeland Security Grant Program and resourcing for national preparedness under the Federal Emergency Management Agency are well-established, the United States Government has no equivalent for cybersecurity preparation or prevention;

(8) the lack of a consistent, resourced fund for investing in resilience in key areas inhibits the United States Government from conveying its understanding of risk into strategy, planning, and action in furtherance of core objectives for the security and resilience of critical infrastructure;

(9) Congress has worked diligently to establish the Cybersecurity and Infrastructure Security Agency, creating a new agency that can leverage broad authorities to receive and share information, provide technical assistance to operators, and partner with stakeholders across the executive branch, State and local communities, and the private sector;

(10) the Cybersecurity and Infrastructure Security Agency requires strengthening in its mission to ensure the national resilience of critical infrastructure, promote a more secure cyber ecosystem, and serve as the central coordinating element to support and integrate Federal, State, local, and private-sector cybersecurity efforts; and

(11) the Cybersecurity and Infrastructure Security Agency requires further resource investment and clear authorities to realize its full potential.

(b) 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 2202(c) (6 U.S.C. 652(c))—

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

(B) in the first paragraph designated as paragraph (12), relating to the Cybersecurity State Coordinator—

(i) by striking ''section 2215'' and inserting ''section 2217''; and

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

(C) by redesignating the second and third paragraphs designated as paragraph (12) as paragraphs (13) and (14), respectively;

(2) by redesignating section 2217 (6 U.S.C. 665f) as section 2220;

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

(4) by redesignating the fourth section 2215 (relating to Sector Risk Management Agencies) (6 U.S.C. 665d) as section 2218;

(5) by redesignating the third section 2215 (relating to the Cybersecurity State Coordinator) (6 U.S.C. 665c) as section 2217;

(6) by redesignating the second section 2215 (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 CYBER RESILIENCE ASSISTANCE FUND.

''(a) DEFINITIONS.—In this section:

''(1) CYBERSECURITY RISK.—The term 'cybersecurity risk' has the meaning given that term in section 2209.

''(2) ELIGIBLE ENTITY.—The term 'eligible entity' means an entity that meets the guidelines and requirements for eligible entities established by the Secretary under subsection (d)(4).

''(3) FUND.—The term 'Fund' means the National Cyber Resilience Assistance Fund established under subsection (c).

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

''(b) CREATION OF A CRITICAL INFRASTRUCTURE RESILIENCE STRATEGY AND A NATIONAL RISK MANAGEMENT CYCLE.—

''(1) INITIAL RISK IDENTIFICATION AND ASSESSMENT.—

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

''(B) CONSULTATION.—In establishing the process required under subparagraph (A), the Secretary shall consult with Sector Risk Management Agencies, critical infrastructure owners

and operators, 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).

''(D) REPORT.—Not later than 1 year after the date of enactment of this section, 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).

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

''(A) IN GENERAL.—Not later than 1 year after the date on which the Secretary delivers the report required under paragraph (1)(D), the President shall deliver to majority and minority leaders of the Senate, the Speaker and minority leader of the House of Representatives, the Committee on Homeland Security and

Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a national critical infrastructure resilience strategy designed to address the risks identified by the Secretary.

''(B) ELEMENTS.—In the strategy delivered under subparagraph (A), the President shall—

''(i) identify, assess, and prioritize areas of risk to critical infrastructure that would compromise, disrupt, or impede the ability of the critical infrastructure to support the national critical functions of national security, economic security, or public health and safety;

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

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

''(iv) outline the budget plan required to provide sufficient resources to successfully execute the full range of activities proposed or described by the strategy; and

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

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

''(3) CONGRESSIONAL BRIEFING.—Not later than 1 year after the date on which the President delivers the strategy under subparagraph (A), and every year thereafter, the Secretary, in coordination with Sector Risk Management Agencies, shall brief the appropriate congressional committees on the national risk management cycle activities undertaken pursuant to the strategy.

''(4) FIVE YEAR RISK MANAGEMENT CYCLE.—

''(A) RISK IDENTIFICATION AND ASSESSMENT.—Under procedures established by the Secretary, the Secretary shall repeat the conducting and reporting of the risk identification and assessment required under paragraph (1),

in accordance with the requirements in paragraph (1), every 5 years.

''(B) STRATEGY.—Under procedures established by the President, the President shall repeat the preparation and delivery of the critical infrastructure resilience strategy required under paragraph (2), in accordance with the requirements in paragraph (2), every 5 years, which shall also include assessing the implementation of the previous national critical infrastructure resilience strategy.

''(c) ESTABLISHMENT OF THE NATIONAL CYBER RESILIENCE ASSISTANCE FUND.—There is established in the Treasury of the United States a fund, to be known as the 'National Cyber Resilience Assistance Fund', which shall be available for the cost of risk-based grant programs focused on systematically increasing the resilience of public and private critical infrastructure against cybersecurity risk, thereby increasing the overall resilience of the United States.

''(d) ADMINISTRATION OF GRANTS FROM THE NATIONAL CYBER RESILIENCE ASSISTANCE FUND.—

''(1) IN GENERAL.—In accordance with this section, the Secretary, acting through the Administrator of the Federal Emergency Management Agen-

cy and the Director, shall develop and administer processes to—

"(A) establish focused grant programs to address identified areas of cybersecurity risk to, and bolster the resilience of, critical infrastructure;

"(B) accept and evaluate applications for each such grant program;

"(C) award grants under each such grant program; and

"(D) disburse amounts from the Fund.

"(2) ESTABLISHMENT OF RISK-FOCUSED GRANT PROGRAMS.—

"(A) ESTABLISHMENT.—

"(i) IN GENERAL.—The Secretary, acting through the Director and the Administrator of the Federal Emergency Management Agency, may establish not less than 1 grant program focused on mitigating an identified category of cybersecurity risk identified under the national risk management cycle and critical infrastructure resilience strategy under subsection (b) in order to bolster the resilience of crit-

ical infrastructure within the United States.

"(ii) SELECTION OF FOCUS AREA.—Before selecting a focus area for a grant program pursuant to this subparagraph, the Director shall ensure—

"(I) there is a clearly defined cybersecurity risk identified through the national risk management cycle and critical infrastructure resilience strategy under subsection (b) to be mitigated;

"(II) market forces do not provide sufficient private-sector incentives to mitigate the risk without Government investment; and

"(III) there is clear Federal need, role, and responsibility to mitigate the risk in order to bolster the resilience of critical infrastructure.

"(B) FUNDING.—

"(i) RECOMMENDATION.—Beginning in the first fiscal year following the establishment of the Fund and each fiscal year thereafter, the Director shall—

''(I) assess the funds available in the Fund for the fiscal year; and

''(II) recommend to the Secretary the total amount to be made available from the Fund under each grant program established under this subsection.

''(ii) ALLOCATION.—After considering the recommendations made by the Director under clause (i) for a fiscal year, the Director shall allocate amounts from the Fund to each active grant program established under this subsection for the fiscal year.

''(3) USE OF FUNDS.—Amounts in the Fund shall be used to mitigate risks identified through the national risk management cycle and critical infrastructure resilience strategy under subsection (b).

''(4) ELIGIBLE ENTITIES.—

''(A) GUIDELINES AND REQUIREMENTS.—

''(i) IN GENERAL.—In accordance with clause (ii), the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate

and the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives a set of guidelines and requirements for determining the entities that are eligible entities.

''(ii) DEADLINES.—The Secretary shall submit the guidelines and requirements under clause (i)—

''(I) not later than 180 days after the date of enactment of this section, and every 2 years thereafter; and

''(II) not later than 30 days before the date on which the Secretary implements the guidelines and requirements.

''(B) CONSIDERATIONS.—In developing guidelines and requirements for eligible entities under subparagraph (A), the Secretary shall consider—

''(i) number of employees;

''(ii) annual revenue;

''(iii) existing entity cybersecurity spending;

"(iv) current cyber risk assessments, including credible threats, vulnerabilities, and consequences; and

"(v) entity capacity to invest in mitigating cybersecurity risk absent assistance from the Federal Government.

"(5) LIMITATION.—For any fiscal year, an eligible entity may not receive more than 1 grant from each grant program established under this subsection.

"(6) GRANT PROCESSES.—The Secretary, acting through the Administrator of the Federal Emergency Management Agency, shall require the submission of such information as the Secretary determines is necessary to—

"(A) evaluate a grant application against the criteria established under this section;

"(B) disburse grant funds;

"(C) provide oversight of disbursed grant funds; and

"(D) evaluate the effectiveness of the funded project in increasing the overall resilience of the United States with respect to cybersecurity risks.

''(7) GRANT CRITERIA.—For each grant program established under this subsection, the Director, in coordination with the Administrator of the Federal Emergency Management Agency, shall develop and publish criteria for evaluating applications for funding, which shall include—

''(A) whether the application identifies a clearly defined cybersecurity risk;

''(B) whether the cybersecurity risk identified in the grant application poses a substantial threat to critical infrastructure;

''(C) whether the application identifies a program or project clearly designed to mitigate a cybersecurity risk;

''(D) the potential consequences of leaving the identified cybersecurity risk unmitigated, including the potential impact to the critical functions and overall resilience of the nation; and

''(E) other appropriate factors identified by the Director.

''(8) EVALUATION OF GRANTS APPLICATIONS.—

''(A) IN GENERAL.—Utilizing the criteria established under paragraph (7), the Director, in coordination with the Administrator of the Federal Emergency Management Agency, shall

evaluate grant applications made under each grant program established under this subsection.

"(B) RECOMMENDATION.—Following the evaluations required under subparagraph (A), the Director shall recommend to the Secretary applications for approval, including the amount of funding recommended for each such approval.

"(9) AWARD OF GRANT FUNDING.—The Secretary shall—

"(A) review the recommendations of the Director prepared pursuant to paragraph (8); and

"(B) provide a final determination of grant awards to the Administrator of the Federal Emergency Management Agency to be disbursed and administered under the process established under paragraph (6).

"(e) EVALUATION OF GRANT PROGRAMS UTILIZING THE NATIONAL CYBER RESILIENCE ASSISTANCE FUND.—

"(1) EVALUATION.—The Secretary shall establish a process to evaluate the effectiveness and efficiency of grants distributed under this section and

develop appropriate updates, as needed, to the grant programs.

''(2) ANNUAL REPORT.—Not later than 180 days after the conclusion of the first fiscal year in which grants are awarded under this section, and every fiscal year thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives a report detailing the grants awarded from the Fund, the status of projects undertaken with the grant funds, any planned changes to the disbursement methodology of the Fund, measurements of success, and total outlays from the Fund.

''(3) GRANT PROGRAM REVIEW.—

''(A) ANNUAL ASSESSMENT.—Before the start of the second fiscal year in which grants are awarded under this section, and every fiscal year thereafter, the Director shall assess the grant programs established under this section and determine—

''(i) for the coming fiscal year—

''(I) whether new grant programs with additional focus areas should be created;

''(II) whether any existing grant program should be discontinued; and

''(III) whether the scope of any existing grant program should be modified; and

''(ii) the success of the grant programs in the prior fiscal year.

''(B) SUBMISSION TO CONGRESS.—Not later than 90 days before the start of the second fiscal year in which grants are awarded under this section, and every fiscal year thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives the assessment conducted pursuant to subparagraph (A) and any planned alterations to the grant program for the coming fiscal year.

''(f) LIMITATION ON USE OF GRANT FUNDS.—Funds awarded pursuant to this section—

''(1) shall supplement and not supplant State or local funds or, as applicable, funds supplied by the Bureau of Indian Affairs; and

''(2) may not be used—

''(A) to provide any Federal cost-sharing contribution on behalf of a State or local government;

''(B) to pay a ransom;

''(C) by or for a non-United States entity; or

''(D) for any recreational or social purpose.

''(g) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section $75,000,000 for each of fiscal years 2022 through 2026.

''(h) TRANSFERS AUTHORIZED.—During a fiscal year, the Secretary or the head of any component of the Department that administers the State and Local Cybersecurity Grant Program may transfer not more than 5 percent of the amounts appropriated pursuant to subsection (g) or other amounts appropriated to carry out the National Cyber Resilience Assistance Fund for that fiscal year to an account of the Department for salaries, expenses, and other administrative costs incurred for the management, administration, or evaluation of this section.''.

(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 striking the item relating to section 2214 and all that follows through the item relating to section 2217 and inserting the following:

"Sec. 2214. 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.
"Sec. 2220A. National Cyber Resilience Assistance Fund.".

(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 II—IMPROVING THE ABILITY OF THE FEDERAL GOVERNMENT TO ASSIST IN ENHANCING CRITICAL INFRASTRUCTURE CYBER RESILIENCE

SEC. 201. INSTITUTE A 5-YEAR TERM FOR THE CYBERSECURITY AND INFRASTRUCTURE SECURITY DIRECTOR.

(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 Director shall be appointed for a term of 5 years.'' after ''who shall report to the Secretary.''.

(b) TRANSITION RULES.—The amendment made by subsection (a) shall take effect on the earlier of—

(1) the first appointment of an individual to the position of Director of the Cybersecurity and Infrastructure Protection Agency of the Department of Homeland Security, by and with the advice and consent of the Senate, that is made on or after the date of enactment of this Act; or

(2) January 1, 2022.

SEC. 202. CREATE A JOINT COLLABORATIVE ENVIRONMENT.

(a) IN GENERAL.—The Director of the Cybersecurity and Infrastructure Security Agency shall establish a joint, cloud-based, information sharing environment to—

(1) integrate the Federal Government's unclassified and classified cyber threat information, malware forensics, and data related to cybersecurity risks (as defined in section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659)) that is derived from network sensor programs;

(2) enable cross-correlation of threat data at the speed and scale necessary for rapid detection and identification;

(3) enable query and analysis by appropriate operators across the Federal Government;

(4) facilitate a whole-of-Government, comprehensive understanding of the cyber threats to the resilience of the Federal Government and national critical infrastructure networks;

(5) enable and support the private-public cybersecurity collaboration efforts of the Federal Government, whose successes will be directly dependent on the accuracy, comprehensiveness, and timeliness of threat information collected and held by the Federal Government; and

(6) enable data curation for artificial intelligence models and provide an environment to enable the Federal Government to curate data and build applications.

(b) DEVELOPMENT.—

(1) INITIAL EVALUATION.—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—

(A) identify all Federal sources of classified and unclassified cyber threat information;

(B) evaluate all programs, applications, or platforms of the Federal Government that are intended to detect, identify, analyze, or monitor cyber threats against the resiliency of the Federal Government or critical infrastructure; and

(C) submit a recommendation to the President identifying Federal programs to be designated and required to participate in the Information Sharing Environment, including—

(i) Government network-monitoring and intrusion detection programs;

(ii) cyber threat indicator-sharing programs and Government-sponsored network

sensors or network-monitoring programs for the private sector or for State, local, tribal, and territorial governments;

(iii) incident response and cybersecurity technical assistance programs; and

(iv) malware forensics and reverse-engineering programs.

(2) DESIGNATION OF PARTICIPATING PROGRAMS.—Not later than 60 days after completion of the evaluation required under paragraph (1), the President shall issue a determination designating the departments, agencies, Federal programs, and corresponding systems and assets that are required to be a part of the Information Sharing Environment.

(3) DESIGN.—Not later than 1 year after completion of the evaluation required under paragraph (1), the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director, shall design the structure of a common platform for sharing and fusing existing Government information, insights, and data related to cyber threats and threat actors, which, at a minimum, shall—

(A) account for appropriate data standards and interoperability requirements;

(B) enable integration of existing applications, platforms, data, and information, to include classified information;

(C) ensure access by such Federal departments and agencies as the Director of the Cybersecurity and Infrastructure Security Agency determines necessary;

(D) account for potential private sector participation and partnerships;

(E) enable unclassified data to be integrated with classified data;

(F) anticipate the deployment of analytic tools across classification levels to leverage all relevant data sets, as appropriate;

(G) identify tools and analytical software that can be applied and shared to manipulate, transform, and display data and other identified needs;

(H) anticipate the integration of new technologies and data streams, including data related to cybersecurity risks derived from Government-sponsored voluntary network sensors or network-monitoring programs for the private sector or for State, local, Tribal, and territorial governments; and

(I) appropriately account for departments, agencies, programs, and systems and assets determined to be required to participate by the President under paragraph (2) in the Information Sharing Environment.

(c) OPERATION.—The Information Sharing Environment shall be managed by the Director of the Cybersecurity and Infrastructure Security Agency.

(d) POST-DEPLOYMENT ASSESSMENT.—Not later than 1 year after the date on which the Information Sharing Environment is established, the Director of the Cybersecurity and Infrastructure Security Agency and the Director shall assess the means by which the Information Sharing Environment may be expanded to include the private sector and critical infrastructure information sharing organizations and, to the maximum extent practicable, begin the process of such expansion.

(e) PRIVATE SECTOR SHARING INFORMATION SHARING PROTECTIONS.—To the extent any private entity shares cyber threat indicators and defensive measures through or with the Information Sharing Environment and in a manner that is consistent with all requirements under section 1752 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500), the Cybersecurity Information Sharing

Act of 2015 (6 U.S.C. 1501 et seq.), and any applicable guidelines promulgated under subsection (f), such activities shall be considered to be authorized by and in accordance with section 1752 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 and the Cybersecurity Information Sharing Act of 2015.

(f) PRIVACY AND CIVIL LIBERTIES.—

(1) GUIDELINES OF ATTORNEY GENERAL.—Not later than 60 days after the date of enactment of this Act, the Secretary of Homeland Security (acting through the Director of the Cybersecurity and Infrastructure Security Agency) and the Attorney General, shall jointly, and in coordination with heads of the appropriate Federal entities and in consultation with officers designated under section 1062 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee–1), develop, submit to Congress, and make available to the public interim guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this section.

(2) FINAL GUIDELINES.—

(A) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Secretary of Homeland Security (acting through the Director of the Cybersecurity and Infrastructure Security Agency) and the Attorney General, shall jointly, in coordination with heads of the appropriate Federal entities and in consultation with officers designated under section 1062 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee–1) and such private entities with industry expertise as the Secretary and the Attorney General consider relevant, promulgate final guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this section.

(B) PERIODIC REVIEW.—The Secretary of Homeland Security (acting through the Director of the Cybersecurity and Infrastructure Security Agency) and the Attorney General, shall jointly, in coordination with heads of the appropriate Federal entities and in consultation with officers and private entities described in sub-

paragraph (A), periodically, but not less frequently than once every 2 years, review the guidelines promulgated under subparagraph (A).

(3) CONTENT.—The guidelines required by paragraphs (1) and (2) shall, consistent with the need to bolster the resilience of information systems and mitigate cybersecurity threats—

(A) limit the effect on privacy and civil liberties of activities by the Federal Government under this section;

(B) limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information or information that identifies specific persons, including by establishing—

(i) a process for the timely destruction of such information that is known not to be directly related to uses authorized under this section; and

(ii) specific limitations on the length of any period in which a cyber threat indicator may be retained;

(C) include requirements to safeguard cyber threat indicators containing personal in-

formation or information that identifies specific persons from unauthorized access or acquisition, including appropriate sanctions for activities by officers, employees, or agents of the Federal Government in contravention of such guidelines;

(D) include procedures for notifying entities and Federal entities if information received pursuant to this subsection is known or determined by a Federal entity receiving such information not to constitute a cyber threat indicator;

(E) protect the confidentiality of cyber threat indicators containing personal information or information that identifies specific persons to the greatest extent practicable and require recipients to be informed that such indicators may only be used for purposes authorized under this section; and

(F) include steps that may be needed so that dissemination of cyber threat indicators is consistent with the protection of classified and other sensitive national security information.

(g) OVERSIGHT OF GOVERNMENT ACTIVITIES.—

(1) BIENNIAL REPORT ON PRIVACY AND CIVIL LIBERTIES.—Not later than 2 years after the date of enactment of this Act, and not less frequently than once every year thereafter, the Privacy and Civil Liberties Oversight Board shall submit to Congress and the President a report providing—

(A) an assessment of the effect on privacy and civil liberties by the type of activities carried out under this section; and

(B) an assessment of the sufficiency of the guidelines established pursuant to subsection (f) in addressing concerns relating to privacy and civil liberties.

(2) BIENNIAL REPORT BY INSPECTORS GENERAL.—

(A) IN GENERAL.—Not later than 2 years after the date of enactment of this Act, and not less frequently than once every 2 years thereafter, the Inspector General of the Department of Homeland Security, the Inspector General of the Intelligence Community, the Inspector General of the Department of Justice, the Inspector General of the Department of Defense, and the Inspector General of the Department of Energy shall, in consultation with the Council of In-

spectors General on Integrity and Efficiency, jointly submit to Congress a report on the receipt, use, and dissemination of cyber threat indicators and defensive measures that have been shared with Federal entities under this section.

(B) CONTENTS.—Each report submitted under subparagraph (A) shall include the following:

(i) A review of the types of cyber threat indicators shared with Federal entities.

(ii) A review of the actions taken by Federal entities as a result of the receipt of such cyber threat indicators.

(iii) A list of Federal entities receiving such cyber threat indicators.

(iv) A review of the sharing of such cyber threat indicators among Federal entities to identify inappropriate barriers to sharing information.

(3) RECOMMENDATIONS.—Each report submitted under this subsection may include such recommendations as the Privacy and Civil Liberties Oversight Board, with respect to a report submitted under paragraph (1), or the Inspectors General re-

ferred to in paragraph (2)(A), with respect to a report submitted under paragraph (2), may have for improvements or modifications to the authorities under this section.

(4) FORM.—Each report required under this subsection shall be submitted in unclassified form, but may include a classified annex.

(h) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section $100,000,000 for each of fiscal years 2022 through 2026.

(i) DEFINITIONS.—In this section:

(1) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' has the meaning given that term in section 1016(e) of the Critical Infrastructure Protection Act of 2001 (42 U.S.C. 5195c(e)).

(2) DIRECTOR.—The term ''Director'' means the National Cyber Director.

(3) INFORMATION SHARING ENVIRONMENT.—The term ''Information Sharing Environment'' means the information sharing environment established under subsection (a).

SEC. 203. DESIGNATE THREE CRITICAL TECHNOLOGY SECURITY CENTERS.

(a) IN GENERAL.—Section 307(b)(3) of the Homeland Security Act of 2002 (6 U.S.C. 187(b)(3)), is amended—

(1) in the matter preceding subparagraph (A), by inserting ''national laboratories,'' before ''and universities'';

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

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

(4) by adding at the end the following:

''(E) establish not less than 1, and not more than 3, cybersecurity-focused critical technology security centers, in order to bolster the overall resilience of the networks and critical infrastructure of the United States, to perform—

''(i) network technology security testing, to test the security of cyber-related hardware and software;

''(ii) connected industrial control system security testing, to test the security of connected programmable data logic controllers, supervisory control and data ac-

quisition servers, and other cyber connected industrial equipment; and

''(iii) open source software security testing, to test and coordinate efforts to fix vulnerabilities in open-source software.''.

(b) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out the amendments made by this section $15,000,000 for each of fiscal years 2022 through 2026.

TITLE III—IMPROVING SECURITY IN THE NATIONAL CYBER ECOSYSTEM

SEC. 301. ESTABLISH A NATIONAL CYBERSECURITY CERTIFICATION AND LABELING AUTHORITY.

(a) DEFINITIONS.—In this section:

(1) ACCREDITED CERTIFYING AGENT.—The term ''accredited certifying agent'' means any person who is accredited by the Authority as a certifying agent for the purposes of certifying a specific class of critical information and communications technology.

(2) AUTHORITY.—The term ''Authority'' means the National Cybersecurity Certification and Labeling Authority established under subsection (b)(1).

(3) CERTIFICATION.—The term ''certification'' means a seal or symbol provided by the Authority or an accredited certifying agent, that results from passage of a comprehensive evaluation of an information and communications technology that establishes the extent to which a particular design and implementation meets a set of specified security standards.

(4) CRITICAL INFORMATION AND COMMUNICATIONS TECHNOLOGY.—The term ''critical information and communications technology'' means information and communications technology that is in use in critical infrastructure sectors and that underpins the resilience of national critical functions, as determined by the Secretary.

(5) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' has the meaning given that term in section 1016(e) of the Critical Infrastructure Protection Act of 2001 (42 U.S.C. 5195c(e)).

(6) LABEL.—The term ''label'' means a clear, visual, and easy to understand symbol or list that conveys specific information about a product's security attributes, characteristics, functionality, components, or other features.

(7) PROGRAM.—The term ''Program'' means the program administered under subsection (b)(1).

(8) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

(b) NATIONAL CYBERSECURITY CERTIFICATION AND LABELING AUTHORITY.—

(1) ESTABLISHMENT.—There is established a National Cybersecurity Certification and Labeling Authority for the purpose of establishing and administering a voluntary national cybersecurity certification and labeling program for critical information and communications technology in order to bolster the resilience of the networks and critical infrastructure of the United States.

(2) PROGRAMS.—

(A) ACCREDITATION OF CERTIFYING AGENTS.—As part of the Program, the Authority shall define and publish a process whereby governmental and nongovernmental entities may apply to become accredited certifying agents for the certification of specific critical information and communications technology, including—

(i) smartphones;

(ii) tablets;

(iii) laptop computers;

(iv) operating systems;

(v) routers;

(vi) software-as-a-service;

(vii) infrastructure-as-a-service;

(viii) platform-as-a-service;

(ix) programmable logic controllers;

(x) intelligent electronic devices; and

(xi) programmable automation controllers.

(B) IDENTIFICATION OF STANDARDS, FRAMEWORKS, AND BENCHMARKS.—As part of the Program, the Authority shall work in coordination with accredited certifying agents, the Secretary, and subject matter experts from the Federal Government, academia, nongovernmental organizations, and the private sector to identify and harmonize common security standards, frameworks, and benchmarks against which the security of critical information and communications technologies may be measured.

(C) PRODUCT CERTIFICATION.—As part of the Program, the Authority, in consultation with the Secretary and other experts from the Federal Government, academia, nongovern-

mental organizations, and the private sector, shall—

(i) develop, and disseminate to accredited certifying agents, guidelines to standardize the presentation of certifications to communicate the level of security for critical information and communications technologies;

(ii) develop, or permit accredited certifying agents to develop, certification criteria for critical information and communications technologies based on identified security standards, frameworks, and benchmarks, through the work conducted under subparagraph (B);

(iii) issue, or permit accredited certifying agents to issue, certifications for critical information and communications technology that meet and comply with security standards, frameworks, and benchmarks identified through the work conducted under subparagraph (B);

(iv) permit a manufacturer or distributor of critical information and communications technology to display a certificate

reflecting the extent to which the critical information and communications technology meets security standards, frameworks, and benchmarks identified through the work conducted under subparagraph (B);

(v) remove the certification of a critical information and communications technology as a critical information and communications technology certified under the Program if the manufacturer of the certified critical information and communications technology falls out of conformity with the benchmarks security standards, frameworks, or benchmarks identified through the work conducted under subparagraph (B) for the critical information and communications technology;

(vi) work to enhance public awareness of the certification and labeling efforts of the Authority and accredited certifying agents, including through public outreach, education, research and development, and other means; and

(vii) publicly display a list of labels and certified critical information and communications technology, along with their respective certification information.

(D) CERTIFICATIONS.—

(i) IN GENERAL.—A certification shall remain valid for 1 year from the date of issuance.

(ii) CLASSES OF CERTIFICATION.—In developing the guidelines and criteria required under subparagraph (C)(i), the Authority shall designate at least 3 classes of certifications, including the following:

(I) For critical information and communications technology which the product manufacturer or service provider attests meets the criteria for a certification, attestation-based certification.

(II) For critical information and communications technology products and services that have undergone third-party accreditation of criteria for certification, accreditation-based certification.

(III) For critical information and communications technology that has undergone a security evaluation and testing process by a qualifying third party, as determined by the Authority, test-based certification.

(E) PRODUCT LABELING.—The Authority, in consultation with the Secretary and other experts from the Federal Government, academia, nongovernmental organizations, and the private sector, shall—

(i) collaborate with the private sector to standardize language and define a labeling schema to provide transparent information on the security characteristics and constituent components of a software or hardware product; and

(ii) establish a mechanism by which product developers can provide this information for both product labeling and public posting.

(3) ENFORCEMENT.—

(A) IN GENERAL.—It shall be unlawful for a product manufacturer, distributor, or seller to—

(i) falsely attest to, or falsify an audit or test for, a security standard, framework, or benchmark for certification;

(ii) intentionally mislabel a product; or

(iii) fail to maintain the security standard, framework, or benchmark to which the manufacturer, distributor, or seller attested.

(B) ENFORCEMENT BY FEDERAL TRADE COMMISSION.—

(i) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of subparagraph (A) shall be treated as an unfair and deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.

(ii) POWERS OF COMMISSION.—

(I) IN GENERAL.—The Federal Trade Commission shall enforce this paragraph in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though

all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this paragraph.

(II) PRIVILEGES AND IMMUNITIES.—Any person who violates this paragraph shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(c) SELECTION OF THE AUTHORITY.—

(1) SELECTION.—The Secretary shall issue a notice of funding opportunity and select, on a competitive basis, a nonprofit, nongovernmental organization to serve as the Authority for a period of 5 years.

(2) ELIGIBILITY FOR SELECTION.—The Secretary may only select an organization to serve as the Authority if such organization—

(A) is a nongovernmental, nonprofit organization that is—

(i) exempt from taxation under section 501(a) of the Internal Revenue Code of 1986; and

(ii) described in sections 501(c)(3) and 170(b)(1)(A)(vi) of that Code;

(B) has a demonstrable track record of work on cybersecurity and information security standards, frameworks, and benchmarks; and

(C) possesses requisite staffing and expertise, with demonstrable prior experience in technology security or safety standards, frameworks, and benchmarks, as well as certification.

(3) APPLICATION.—The Secretary shall establish a process by which a nonprofit, nongovernmental organization that seeks to be selected as the Authority may apply for consideration.

(4) PROGRAM EVALUATION.—Not later than the date that is 4 years after the initial selection pursuant paragraph (1), and every 4 years thereafter, the Secretary shall—

(A) assess the effectiveness of the labels and certificates produced by the Authority, including—

(i) assessing the costs to businesses that manufacture critical information and

communications technology participating in the Program;

(ii) evaluating the level of participation in the Program by businesses that manufacture critical information and communications technology; and

(iii) assessing the level of public awareness and consumer awareness of the label;

(B) audit the impartiality and fairness of the Authority's activities conducted under this section;

(C) issue a public report on the assessment most recently carried out under subparagraph (A) and the audit most recently carried out under subparagraph (B); and

(D) brief Congress on the findings of the Secretary with respect to the most recent assessment under subparagraph (A) and the most recent audit under subparagraph (B).

(5) RENEWAL.—After the initial selection pursuant to paragraph (1), the Secretary shall, every 5 years—

(A) accept applications from nonprofit, nongovernmental organizations seeking selection as the Authority; and

(B) following competitive consideration of all applications—

(i) renew the selection of the organization serving as the Authority; or

(ii) select another applicant organization to serve as the Authority.

(d) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section $25,000,000 for each of fiscal years 2022 through 2026.

SEC. 302. ESTABLISH THE BUREAU OF CYBERSECURITY STATISTICS.

(a) DEFINITIONS.—In this section:

(1) BUREAU.—The term ''Bureau'' means the Bureau of Cybersecurity Statistics established under subsection (b).

(2) COVERED ENTITY.—The term ''covered entity'' means any nongovernmental organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture (without regard to whether it is established for profit) that is engaged in or affecting interstate commerce and that

provides cybersecurity incident response services or cybersecurity insurance products.

(3) CYBER INCIDENT.—The term cyber incident includes each of the following:

(A) Unauthorized access to an information system or network that leads to loss of confidentiality, integrity, or availability of that information system or network.

(B) Disruption of business operations due to a distributed denial of service attack against an information system or network.

(C) Unauthorized access or disruption of business operations due to loss of service facilitated through, or caused by a cloud service provider, managed service provider, or other data hosting provider.

(D) Fraudulent or malicious use of a cloud service account, data hosting account, internet service account, or any other digital service.

(4) DIRECTOR.—The term ''Director'' means the Director of the Bureau.

(5) STATISTICAL PURPOSE.—The term ''statistical purpose''—

(A) means the description, estimation, or analysis of the characteristics of groups, with-

out identifying the individuals or organizations that comprise such groups; and

(B) includes the development, implementation, or maintenance of methods, technical or administrative procedures, or information resources that support the purposes described in subsection (e).

(b) ESTABLISHMENT.—There is established within the Department of Homeland Security a Bureau of Cybersecurity Statistics.

(c) DIRECTOR.—

(1) IN GENERAL.—The Bureau shall be headed by a Director, who shall—

(A) report to the Secretary of Homeland Security; and

(B) be appointed by the President.

(2) AUTHORITY.—The Director shall—

(A) have final authority for all cooperative agreements and contracts awarded by the Bureau;

(B) be responsible for the integrity of data and statistics collected or issued by the Bureau; and

(C) protect against improper or illegal use or disclosure of information furnished for exclu-

sively statistical purposes under this section, consistent with the requirements of subsection (f).

(3) QUALIFICATIONS.—The Director—

(A) shall have experience in statistical programs; and

(B) shall not—

(i) engage in any other employment; or

(ii) hold any office in, or act in any capacity for, any organization, agency, or institution with which the Bureau makes any contract or other arrangement under this section.

(4) DUTIES AND FUNCTIONS.—The Director shall—

(A) collect and analyze information concerning cybersecurity, including data related to cyber incidents, cyber crime, and any other area the Director determines appropriate;

(B) collect and analyze data that will serve as a continuous and comparable national indication of the prevalence, incidents, rates, extent, distribution, and attributes of all relevant cyber incidents, as determined by the Director,

in support of national policy and decision making;

(C) compile, collate, analyze, publish, and disseminate uniform national cyber statistics concerning any area that the Director determines appropriate;

(D) in coordination with the National Institute of Standards and Technology, recommend national standards, metrics, and measurement criteria for cyber statistics and for ensuring the reliability and validity of statistics collected pursuant to this subsection;

(E) conduct or support research relating to methods of gathering or analyzing cyber statistics;

(F) enter into cooperative agreements or contracts with public agencies, institutions of higher education, or private organizations for purposes related to this subsection;

(G) provide appropriate information to the President, the Congress, Federal agencies, the private sector, and the general public on cyber statistics;

(H) maintain liaison with State and local governments concerning cyber statistics;

(I) confer and cooperate with Federal statistical agencies as needed to carry out the purposes of this section, including by entering into cooperative data sharing agreements in conformity with all laws and regulations applicable to the disclosure and use of data; and

(J) request from any person or entity information, data, and reports as may be required to carry out the purposes of this subsection.

(d) FURNISHMENT OF INFORMATION, DATA, OR REPORTS BY FEDERAL DEPARTMENTS AND AGENCIES.—Federal departments and agencies requested by the Director to furnish information, data, or reports pursuant to subsection (c)(4)(J) shall provide to the Bureau such information as the Director determines necessary to carry out the purposes of this section.

(e) FURNISHMENT OF CYBER INCIDENT INFORMATION, DATA, OR REPORTS TO THE BUREAU BY THE PRIVATE SECTOR.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, and every 180 days thereafter, each covered entity shall submit to the Bureau a report containing such data and information as the Director determines necessary to carry out the purposes of this section.

(2) DETERMINATION OF DATA AND INFORMATION NECESSARY TO CARRY OUT THE PURPOSES OF THIS SECTION.—Not later than 90 days after the date of enactment of this Act, and annually thereafter, the Director shall publish a list of data and information determined necessary to carry out the purposes of this section, including individual descriptions of cyber incidents, which shall include—

(A) identification of the affected databases, information systems, or devices that were, or are reasonably believed to have been accessed by an unauthorized person;

(B) where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used;

(C) where applicable, any identifying information related to the malicious actors who perpetrated the incident;

(D) where applicable any cybersecurity controls implemented by the victim organization; and

(E) the industrial sectors, regions, and size of affected entities (as determined by number of employees) without providing any information

that can reasonably be expected to identify such entities.

(3) STANDARDS FOR SUBMISSION OF INFORMATION AND DATA.—Not later than 180 days after the date of enactment of this Act, the Director shall, in consultation with covered entities, develop standardized procedures for the submission of data and information the Director determines necessary to carry out the purposes of this section.

(4) PRIVATE SECTOR REPORTING.—Not later than 90 days after the date on which the Director develops the standards required under paragraph (3), the Director shall—

(A) publish the processes for submission of information, data, and reports by covered entities; and

(B) begin accepting reporting required under paragraph (1).

(5) REGULATORY USE.—Information disclosed to the Bureau under this section that is not otherwise available, shall not be used by the Federal Government or any State, local, tribal, or territorial government to sanction or otherwise punish the entity disclosing the information, or the entity in which the cyber incident initially occurred.

(6) PRESERVATION OF PRIVILEGE.—Disclosure of information pursuant to this section or by a covered entity to the Bureau shall not waive any otherwise applicable privilege, immunity, or protection provided by law.

(7) PRESERVATION OF EXISTING OBLIGATIONS.—Nothing in this section shall modify, prevent, or abrogate any notice or notification obligations under Federal contracts, enforceable agreements with the government, or other Federal law.

(8) ENFORCEMENT.—

(A) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—Compliance with the requirements imposed under this subsection by covered entities shall be enforced by the Federal Trade Commission under the Federal Trade Commission Act (15 U.S.C. 41 et seq.). For the purpose of the exercise by the Federal Trade Commission of its functions and powers under the Federal Trade Commission Act, a violation of any requirement or prohibition imposed under this subsection shall be treated as an unfair and deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C.

57a(a)(1)(B)) regarding unfair or deceptive acts or practices.

(B) POWERS OF COMMISSION.—Subject to subparagraph (C), the Federal Trade Commission shall enforce this subsection in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this subsection.

(C) ADDITIONAL ENTITIES.—

(i) IN GENERAL.—Notwithstanding sections 4, 5(a)(2), or 6 of the Federal Trade Commission Act (15 U.S.C. 44, 45(a)(2), 46) or any jurisdictional limitation of the Federal Trade Commission, the Federal Trade Commission shall also enforce this subsection, in the same manner provided in subparagraph (A) of this paragraph, with respect to—

(I) organizations not organized to carry on business for their own profit or that of their members; and

(II) common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.).

(ii) COORDINATION AND NOTICE.—The Federal Trade Commission shall—

(I) coordinate with the Federal Communications Commission regarding enforcement of this subsection with respect to common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.);

(II) notify the Bureau of Consumer Financial Protection regarding enforcement of this subsection with respect to information associated with the provision of financial products or services by an entity that provides a consumer financial product or service (as defined in section 1002 of the Consumer Financial Protection Act of 2010 (12 U.S.C. 5481)); and

(III) for enforcement of this subsection with respect to matters implicating the jurisdiction or authorities

of another Federal agency, notify that agency as appropriate.

(D) PRIVILEGES AND IMMUNITIES.—Any covered entity that violates the requirements imposed under this subsection shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(E) CONSTRUCTION.—Nothing in this paragraph shall be construed to limit the authority of the Federal Trade Commission under any other provision of law.

(f) PROTECTION OF INFORMATION.—

(1) IN GENERAL.—No officer or employee of the Federal Government or agent of the Federal Government may, without the consent of the individual, entity, agency, or other person who is the subject of the submission or provides the submission—

(A) use any submission that is furnished for exclusively statistical purposes under this section for any purpose other than the statistical purposes for which the submission is furnished;

(B) make any publication or media transmittal of the data contained in a submission described in subparagraph (A) that permits information concerning individual entities or individual incidents to be reasonably inferred by either direct or indirect means; or

(C) permit anyone other than a sworn officer, employee, agent, or contractor of the Bureau to examine an individual submission described in subsection (e).

(2) IMMUNITY FROM LEGAL PROCESS.—Any submission (including any data derived from the submission) that is collected and retained by the Bureau, or an officer, employee, agent, or contractor of the Bureau, for exclusively statistical purposes under this section shall be immune from the legal process and shall not, without the consent of the individual, entity, agency, or other person who is the subject of the submission or provides the submission, be admitted as evidence or used for any purpose in any action, suit, or other judicial or administrative proceeding.

(3) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to provide immunity from the legal process for a submission (including

any data derived from the submission) if the submission is in the possession of any person, agency, or entity other than the Bureau or an officers, employee, agent, or contractor of the Bureau, or if the submission is independently collected, retained, or produced for purposes other than the purposes of this section.

(g) AUTHORIZATION OF APPROPRIATION.—There are authorized to be appropriated such sums as may be necessary to carry out this section. Such funds shall remain available until expended.

SEC. 303. SECURE FOUNDATIONAL INTERNET PROTOCOLS.

(a) DEFINITIONS.—In this section:

(1) BORDER GATEWAY PROTOCOL.—The term ''border gateway protocol'' means a protocol designed to optimize routing of information exchanged through the internet.

(2) DOMAIN NAME SYSTEM.—The term ''domain name system'' means a system that stores information associated with domain names in a distributed database on networks.

(3) INFORMATION AND COMMUNICATIONS TECHNOLOGY INFRASTRUCTURE PROVIDERS.—The term ''information and communications technology infrastructure providers'' means all systems that en-

able connectivity and operability of internet service, backbone, cloud, web hosting, content delivery, domain name system, and software-defined networks and other systems and services.

(b) CREATION OF A STRATEGY TO SECURE FOUNDATIONAL INTERNET PROTOCOLS.—

(1) PROTOCOL SECURITY STRATEGY.—In order to secure foundational internet protocols, not later than December 31, 2021, the National Telecommunications and Information Administration and the Department of Homeland Security shall submit to Congress a strategy to secure the border gateway protocol and the domain name system.

(2) STRATEGY REQUIREMENTS.—The strategy required under paragraph (1) shall—

(A) articulate the security and privacy benefits of implementing security for the border gateway protocol and the domain name system and the burdens of implementation and the entities on whom those burdens will most likely fall;

(B) identify key United States and international stakeholders;

(C) outline identified security measures that could be used to secure or provide authen-

tication for the border gateway protocol and the domain name system;

(D) identify any barriers to implementing security for the border gateway protocol and the domain name system at scale;

(E) propose a strategy to implement identified security measures at scale, accounting for barriers to implementation and balancing benefits and burdens, where feasible; and

(F) provide an initial estimate of the total cost to the Government and implementing entities in the private sector of implementing security for the border gateway protocol and the domain name system and propose recommendations for defraying these costs, if applicable.

(3) CONSULTATION.—In developing the strategy required under paragraph (1) the National Telecommunications and Information Administration and the Department of Homeland Security shall consult with information and communications technology infrastructure providers, civil society organizations, relevant nonprofit organizations, and academic experts.

TITLE IV—SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE

SEC. 401. DEFINITIONS.

In this title:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives.

(2) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' has the meaning given that term in section 1016(e) of the Critical Infrastructure Protection Act of 2001 (42 U.S.C. 5195c(e)).

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

(4) ENTITY.—The term ''entity'' means a non-Federal entity and a private entity, as such terms are defined under section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

(5) NATIONAL CRITICAL FUNCTIONS.—The term ''national critical functions'' means functions of government and the private sector so vital to the United States that their disruption, corruption, or

dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

(6) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

(7) STAKEHOLDERS.—The term ''stakeholders'' means persons or groups whose consultation may aid the Secretary in exercising the authority of the Secretary under this title, including—

(A) Sector Coordinating Councils within the Critical Infrastructure Partnership Advisory Council, established under section 871 of the Homeland Security Act of 2002 (6 U.S.C. 451);

(B) the State, Local, Tribal and Territorial Government Coordinating Council, within the Critical Infrastructure Partnership Advisory Council, established under section 871 of the Homeland Security Act of 2002 (6.U.S.C. 451);

(C) the Cybersecurity Advisory Committee established under section 2219 of the Homeland Security Act of 2002 (6 U.S.C. 665e), as so redesignated by section 101 of this Act;

(D) the National Security Telecommunications Advisory Committee established pursu-

ant to Executive Order 12382 (47 Fed. Reg. 40531); and

(E) the National Infrastructure Advisory Council, established pursuant to Executive Order 13231 (66 Fed. Reg. 53063).

(8) SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE.—The term ''Systemically Important Critical Infrastructure'' means an entity that has been designated as such by the Secretary through the process and procedures established under section 402.

SEC. 402. SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE.

(a) IN GENERAL.—The Secretary may designate entities as Systemically Important Critical Infrastructure.

(b) ESTABLISHMENT OF METHODOLOGY AND CRITERIA.—Prior to designating any entities as Systemically Important Critical Infrastructure, the Secretary, in consultation with the National Cyber Director, Sector Risk Management Agencies, and appropriate stakeholders shall develop—

(1) a methodology for identifying Systemically Important Critical Infrastructure; and

(2) criteria for determining whether an entity qualifies as Systemically Important Critical Infrastructure.

(c) CONSIDERATIONS.—In establishing criteria for determining whether an entity qualifies as Systemically Important Critical Infrastructure, the Secretary shall consider—

(1) the likelihood that disruption to or compromise of such an entity could cause a debilitating effect on national security, economic security, public health or safety, or any combination thereof;

(2) the extent to which damage, disruption, or unauthorized access to such an entity either separately or collectively, will disrupt the reliable operation of other critical infrastructure assets, or impede provisioning of one or more national critical functions;

(3) the extent to which national cybersecurity resilience would be enhanced by deeper risk management integration between Systemically Important Critical Infrastructure entities and the Federal Government; and

(4) the extent to which compromise or unauthorized access of such an entity could separately or collectively create widespread compromise of the

cyber ecosystem, significant portions of critical infrastructure, or multiple critical infrastructure sectors.

(d) LIST.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Secretary shall complete an initial list of entities designated as Systemically Important Critical Infrastructure.

(2) MAINTENANCE OF LIST.—The Secretary shall maintain a comprehensive list of entities designated as Systemically Important Critical Infrastructure, which shall be updated within 7 days of a change in whether an entity qualifies as Systemically Important Critical Infrastructure.

(e) ENTITY NOTIFICATIONS.—Not later than 90 days after designating an entity as Systemically Important Critical Infrastructure or removing the designation of an entity as Systemically Important Critical Infrastructure, the Secretary shall notify the entity.

(f) CONGRESSIONAL NOTIFICATIONS.—The Secretary shall—

(1) not later than 30 days after the date of any addition, modification, or removal of an entity from the list of Significantly Important Critical Infrastructure maintained under subsection (d), notify the appropriate Congressional committees; and

(2) at least every 2 years, submit to the appropriate Congressional committees an updated comprehensive list of entities designated as Systemically Important Critical Infrastructure, in conjunction with each plan required pursuant to section 403.

SEC. 403. PLAN FOR ENHANCEMENT OF SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE METHODOLOGY AND CAPABILITY.

(a) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, and every 2 years thereafter for 10 years, the Secretary, in consultation with Sector Risk Management Agencies and appropriate stakeholders, shall develop and submit to the appropriate congressional committees a plan for enhancing the methodology of the Department for identifying Systemically Important Critical Infrastructure, including a discussion of the progress of the Department as of the date of submission of the plan in implementing the plan.

(b) CONTENTS OF PLAN.—

(1) IN GENERAL.—The plan required under subsection (a) shall include—

(A) the methodology and criteria used for identifying and determining entities that qualify as Systemically Important Critical Infrastructure as described in section 402(b) and the

analysis used to establish such methodology and criteria;

(B) a proposed timeline for enhancing the capabilities of the Department to expand the list beyond the designated entities to also include facilities, systems, assets, or other relevant units of critical infrastructure that may further enhance the ability to manage risk of Systemically Important Critical Infrastructure;

(C) information regarding the outreach by the Department to stakeholders and other Sector Risk Management Agencies on such efforts, including mechanisms for incorporation of industry feedback;

(D) information regarding the efforts of the Department, and the associated challenges with such efforts, to access information from stakeholders and other Sector Risk Management Agencies to identify Systemically Important Critical Infrastructure;

(E) information regarding other critical infrastructure entity identification programs within the Department and how they are being incorporated into the overarching process to identify Systemically Important Critical Infrastruc-

ture, which shall include the efforts of the Department under section 9 of Executive Order 13636 (78 Fed. Reg. 11739), the National Infrastructure Prioritization Program, and section 4 of Executive Order 14028 (86 Fed. Reg. 26633);

(F) any identified gaps in authorities or resources required to successfully carry out the process of identifying Systemically Important Critical Infrastructure, including facilities, systems, assets, or other relevant units of critical infrastructure, as well as legislative proposals to address such gaps;

(G) an assessment of potential benefits for entities designated as Systemically Important Critical Infrastructure, which shall include an assessment of—

(i) enhanced intelligence support and information sharing;

(ii) prioritized Federal technical assistance;

(iii) liability protection for entities designated as Systemically Important Critical Infrastructure that conform to identified security standards for damages or

harm directly or indirectly caused by a cyber incident;

(iv) prioritized emergency planning;

(v) benefits described in the final report of the U.S. Cyberspace Solarium Commission, dated March 2020; and

(vi) additional authorizations or resources necessary to implement the benefits assessed under this subparagraph; and

(H) an assessment of potential mechanisms to improve the security of entities designated as Systemically Important Critical Infrastructure, which shall include an assessment of—

(i) risk-based cybersecurity performance standards for all Systemically Important Critical Infrastructure entities, incorporating, to the greatest extent possible, existing industry best practices, standards, and guidelines;

(ii) sector-specific performance standards;

(iii) additional regulations to enhance the security of Systemically Important Critical Infrastructure against cyber risks,

including how to prevent duplicative requirements for already regulated sectors;

(iv) cyber incident reporting requirements for entities designated as Systemically Important Critical Infrastructure; and

(v) additional authorizations or resources necessary to implement the mechanisms to improve the security of Systemically Important Critical Infrastructure assessed under this subparagraph.

(2) INITIAL PLAN.—The initial plan submitted under this section shall include a detailed description of the capabilities of the Department with respect to identifying Systemically Important Critical Infrastructure as they were on the date of enactment of this Act.

(c) CLASSIFIED ANNEX.—The plan shall be in unclassified form, but may include a classified annex, as the Secretary determines necessary.

(d) PUBLICATION.—Not later than 30 days after the date on which the Secretary submits a plan to Congress, the Secretary shall make the plan available to relevant stakeholders.

(e) RESTRICTION.—Subchapter I of chapter 35 of title 44, United States Code, shall not apply to any action to implement this section or to any exercise of the authority of the Secretary pursuant to this section.

TITLE V—ENABLING THE NATIONAL CYBER DIRECTOR

SEC. 501. ESTABLISHMENT OF HIRING AUTHORITIES FOR THE OFFICE OF THE NATIONAL CYBER DIRECTOR.

Section 1752 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116–283) is amended—

(1) in subsection (e)—

(A) in paragraph (1), by inserting ''and in accordance with paragraphs (3) through (7) of this subsection,'' after ''and classification laws,'';

(B) in paragraph (2), by inserting ''notwithstanding paragraphs (3) through (7) of this subsection,'' before ''employ experts'';

(C) by redesignating paragraphs (3) through (8) as paragraphs (8) through (13), respectively; and

(D) by inserting after paragraph (2) the following:

''(3) establish, as positions in the excepted service, such qualified positions in the Office as the Director determines necessary to carry out the responsibilities of the Office, appoint an individual to a qualified position (after taking into consideration the availability of preference eligibles for appointment to the position), and, subject to the requirements of paragraphs (4) and (5), fix the compensation of an individual for service in a qualified position;

''(4) fix the rates of basic pay for any qualified position established under paragraph (3) in relation to the rates of pay provided for employees in comparable positions in the Office, in which the employee occupying the comparable position performs, manages, or supervises functions that execute the mission of the Office, and, subject to the same limitations on maximum rates of pay and consistent with section 5341 of title 5, United States Code, adopt such provisions of that title to provide for prevailing rate systems of basic pay and apply those provisions to qualified positions for employees in or under which the Office may employ individuals described by section 5342(a)(2)(A) of such title;

''(5) employ an officer or employee of the United States or member of the Armed Forces de-

tailed to the staff of the Office on a non-reimbursable basis—

"(A) as jointly agreed to by the heads of the receiving and detailing elements, for a period not to exceed 3 years;

"(B) which shall not be construed to limit any other source of authority for reimbursable or non-reimbursable details; and

"(C) which shall not be considered an augmentation of the appropriations of the receiving element of the Office;

"(6) provide—

"(A) employees in qualified positions compensation (in addition to basic pay), including benefits, incentives, and allowances, consistent with, and not in excess of the level authorized for, comparable positions authorized by title 5, United States Code; and

"(B) employees in a qualified position whose rate of basic pay is fixed under paragraph (4) an allowance under section 5941 of title 5, United States Code, on the same basis and to the same extent as if the employee was an employee covered by such section, including

eligibility conditions, allowance rates, and all other terms and conditions in law or regulation;

''(7) establish a fellowship program to facilitate a talent exchange program between the private sector and the Office to arrange, with the agreement of a private sector organization and the consent of the employee, for the temporary assignment of an employee to the private sector organization, or from the private sector organization to the Office;''; and

(2) in subsection (g)—

(A) by redesignating paragraphs (3) through (6) as paragraphs (4) through (7), respectively;

(B) by inserting after paragraph (2) the following:

''(3) The term 'excepted service' has the meaning given that term in section 2103 of title 5, United States Code.''; and

(3) by adding at the end the following:

''(8) The term 'preference eligible' has the meaning given that term in section 2108(3) of title 5, United States Code.

''(9) The term 'qualified position' means a position, designated by the Director for the purpose of this section, in which the individual occupying such

position performs, manages, or supervises functions that execute the responsibilities of the Office.''.

○