
UNITED STATES OF AMERICA

# CYBERSPACE SOLARIUM COMMISSION

CO-CHAIRMEN

Senator Angus King (I-Maine)

Representative Mike Gallagher (R-Wisconsin)

JULY 2020

## LEGISLATIVE PROPOSALS

# LETTER FROM THE EXECUTIVE DIRECTOR

The 2019 National Defense Authorization Act tasked the Cyberspace Solarium Commission with answering two fundamental questions. First, what strategic approach will best defend the United States against cyberattacks of significant consequences? Second, what policies and legislation are required to implement that strategy? In its March 2020 report, the Commission advocated for a new strategic approach to cybersecurity—layered cyber deterrence—and produced 82 policy and legislative recommendations to support that strategy.

Now, in this document, the Commission's staff provides 54 separate legislative proposals to support the implementation of the strategy of layered cyber deterrence and its associated legislative recommendations. While some of recommendations set forth in the March 2020 report require action by the executive branch; private-sector corporations; State, local, tribal and territorial governments; and ordinary American citizens, we hope these legislative proposals will expedite the implementation process and better prepare the nation to protect itself in cyberspace.

The Commission's staff drew on its own expertise, as well as the support of our general counsel and trusted legal advisors, to produce these proposals. Although the staff regularly consulted the Commissioners during this process, these proposals were not edited or approved by the Commissioners themselves and should be taken as the product of the staff alone.

We have provided this compilation to the staffs of the relevant congressional committees and subcommittees, as well as to the American public, in the hope and expectation of participating in an ongoing dialogue about its content. We are eager to discuss and further refine this language, with the ultimate goal of helping Congress quickly pass the most effective legislation possible.

Mark Montgomery
Executive Director
Cyberspace Solarium Commission

# CONTENTS

## Reform the U.S. Government's Structure and Organization for Cyberspace



## Strengthen Norms and Non-Military Tools



## Promote National Resilience

## Reshape the Cyber Ecosystem toward Greater Security



## Operationalize Cybersecurity Collaboration with the Private Sector

## Preserve and Employ the Military Instrument of Power

## 1.2 Create House Permanent Select and Senate Select Committees on Cybersecurity

Congress should create House Permanent Select and Senate Select Committees on Cybersecurity to consolidate budgetary and legislative jurisdiction over cybersecurity issues, as well as traditional oversight authority.

---

**IN THE SENATE OF THE UNITED STATES**

**RESOLUTION**

Establishing the Select Committee on Cybersecurity.

*Resolved,* That there is hereby established a select committee of the Senate to be known as the Select Committee on Cybersecurity (hereinafter referred to as the "select committee").

**SEC. 1.** (a) The select committee is authorized and directed to oversee and make continuing studies of and recommendations regarding cybersecurity threats to the United States.

(b) The select committee may report by bill or otherwise on matters within its jurisdiction.

**SEC. 2.** In this resolution:

(1) The term "cybersecurity" means the protection or defense of U.S. persons, assets, or interests in cyberspace from cyberattacks.

(2) The term "cybersecurity breach" means an attack via cyberspace, affecting an individual's or organization's use of cyberspace for the purpose of—

(A) compromising the confidentiality, availability, and/or integrity of an information system or data;

(B) disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure; or

(C) destroying the integrity of data or stealing controlled information.

(3) The term "cyberspace" means the global domain within the information environment consisting of the interdependent network of information systems

infrastructures (including the Internet, telecommunications networks, computer systems, and embedded processors and controllers).

**SEC. 3.** (a) The select committee shall be composed of 15 members from the Senate at large, of whom 8 members shall be appointed by the Majority Leader and 7 members shall be appointed by the Minority Leader.

(b) The Majority Leader and Minority Leader, and the chairpersons and ranking members of the Armed Services Committee and Select Committee on Intelligence, shall serve as ex officio, non-voting members of the select committee. As determined by the Majority Leader and Minority Leader, the chairs and ranking members of other committees deemed relevant to cybersecurity shall also be appointed as ex officio, non-voting members of the select committee.

(C) At the beginning of each Congress, the Majority Leader shall select a chairperson of the select committee and the Minority Leader shall select a vice chairperson for the select committee.

**SEC. 4.** The select committee may be organized into subcommittees. Each subcommittee shall have a chairperson and a vice chairperson who are selected by the chairperson and vice chairperson of the select committee, respectively.

**SEC. 5.** The select committee shall have exclusive jurisdiction and consider all proposed legislation, messages, petitions, memorials, and other matters relating to the following:

(1) Domestic and foreign cybersecurity risks (including state-sponsored threats) to the United States, including to—

(A) the computer systems of the United States;

(B) the infrastructure of the United States;

(C) citizens of the United States;

(D) corporations and other businesses in the United States; and

(E) the commerce of the United States.

(2) The development and implementation of national cybersecurity strategies and policies, including those to strengthen the digital ecosystem and improve whole-of-nation cybersecurity resilience.

(3) The activities of any department or agency relating to preventing, protecting against, or responding to cybersecurity threats to the United States, and

relevant incidents or actions unless the activities, relevant incidents, or actions are conducted under authorities in title 10 or title 50, United States Code.

(4) The organization or reorganization of any department or agency to the extent that the organization or reorganization relates to a function or activity involving preventing, protecting against, or responding to cybersecurity threats to the United States, and relevant incidents or actions, unless the function or activity is conducted under authorities in title 10 or title 50, United States Code.

(5) Authorizations for appropriations, both direct and indirect, for preventing, protecting against, or responding to cybersecurity threats to the United States, and relevant incidents or actions, unless the appropriation is for functions or activities conducted under authorities in title 10 or title 50, United States Code.

**SEC. 6.** (a) The select committee is authorized in its discretion—

(1) to make investigations into any matter within its jurisdiction;

(2) to make expenditures from the contingent fund of the Senate;

(3) to employ personnel;

(4) to hold hearings;

(5) to sit and act at any time or place during the sessions, recesses, and adjourned periods of the Senate;

(6) to require, by subpoena or otherwise, the attendance of witnesses and the production of correspondence, books, papers, and documents;

(7) to take depositions and other testimony and authorize employees of the select committee to take depositions and other testimony;

(8) to procure the services of individual consultants, or organizations thereof, in accordance with section 202(i) of the Legislative Reorganization Act of 1946 (2 U.S.C. 4301(i));

(9) with the prior consent of the government department or agency concerned and the Committee on Rules and Administration, to use on a reimbursable basis the services of personnel of any such department or agency;

(10) to make recommendations and report legislation on matters within its jurisdiction; and

(11) to permit any personal representative of the President, designated by the President to serve as a liaison to the select committee, to attend any closed meeting of the select committee.

(b) The chairperson of the select committee or any member thereof may administer oaths to witnesses.

**SEC. 7.** (a) The select committee may only authorize issuance of a subpoena upon an affirmative vote of a majority of the members of the select committee, which vote may not be held before the time that is 48 hours after notice of the request to authorize the issuance of the subpoena is provided to each member of the select committee, absent unanimous consent.

(b) A subpoena authorized by the select committee—

(1) may be issued under the signature of the chairperson, the vice chairperson, or any member of the select committee designated by the chairperson; and

(2) may be served by any person designated by the chairperson, the vice chairperson, or other member signing the subpoena.

**SEC. 8.** The select committee shall obtain from the President and the heads of departments and agencies the information relevant to cybersecurity risks and threats required to ensure that the members of the select committee have complete and current information relating to cybersecurity activities and threats, which may include obtaining written reports reviewing—

(1) the activities carried out by the department or agency concerned to prevent, protect against, or respond to cybersecurity threats;

(2) the cybersecurity threats from within the United States and from foreign countries that are directed at the United States or its interests;

(3) previously conducted or anticipated covert actions relating to cybersecurity; and

(4) any significant cybersecurity breaches that could—

(A) affect the diplomatic, political, economic, or military relations of the United States with other countries or groups; or

(B) impose a major financial cost on the Federal government, citizens of the United States, corporations or other businesses in the United States, or the commerce of the United States.

**SEC. 9.** Each member of the select committee shall have equal and unimpeded access to information collected or otherwise obtained by the select committee.

**SEC. 10.** (a) No employee of the select committee or any person engaged by contract or otherwise to perform services for or at the request of the select committee shall be given access to any classified information by the select committee unless the employee or person has—

(1) agreed in writing and under oath to be bound by the rules of the Senate (including the jurisdiction of the Select Committee on Ethics) and of the select committee as to the security of such information during and after the period of the employment or contractual agreement with the select committee; and

(2) received an appropriate security clearance, as determined by the select committee, in consultation with the Director of National Intelligence.

(b) The type of security clearance to be required in the case of any employee or person described in subsection (a) shall, within the determination of the select committee, in consultation with the Director of National Intelligence, be commensurate with the sensitivity of the classified information to which the employee or person will be given access by the select committee.

**SEC. 11.** (a) The head of each department and agency shall keep the select committee fully and currently informed with respect to cybersecurity activities and threats, including activities to prevent, protect against, or respond to cybersecurity threats and any significant anticipated activities relating to cybersecurity which are the responsibility of or engaged in by the department or agency.

(b) The head of any department or agency involved in any cybersecurity activities shall furnish any information or document in the possession, custody, or control of the department or agency, or person paid by the department or agency, whenever requested by the select committee with respect to any matter within the jurisdiction of the select committee.

(C) The Director of National Intelligence, the Director of the Central Intelligence Agency, the Secretary of Defense, the Secretary of Homeland Security, the Secretary of State, the Director of the Federal Bureau of Investigation, and the Secretary of Commerce shall each submit to the select committee an annual report on cyber threats.

**SEC. 12.** (a) In addition to other committee staff selected by the select committee, the select committee shall hire or appoint one employee for each member of the select committee to serve as the designated representative of the member on the select committee. The select committee shall only hire or appoint an employee chosen by a member of the

select committee for whom the employee will serve as the designated representative on the select committee.

(b) The select committee shall be afforded a supplement to its budget, to be determined by the Committee on Rules and Administration, to allow for the hire of each employee who fills the position of designated representative to the select committee. The designated representative shall have office space and appropriate office equipment in the select committee spaces. Designated personal representatives shall have the same access to committee staff, information, records, and databases as select committee staff, as determined by the chairperson and vice chairperson.

(C) Each designated employee, as authorized by subsection (a), shall meet all the requirements of relevant statutes, Senate rules, and committee security clearance requirements for employment by the select committee.

(d) Of the amounts made available to the select committee for personnel—

(1) not more than 60 percent shall be under the control of the chairperson; and

(2) not less than 40 percent shall be under the control of the vice chairperson.

**SEC. 13.** (a) The select committee shall adopt rules (not inconsistent with the rules of the Senate and in accordance with rule XXVI of the Standing Rules of the Senate) governing the procedure of the select committee, which shall include addressing how often the select committee shall meet, meeting times and location, type of notifications, notices of hearings, duration of the select committee, and records of the select committee after committee activities are complete.

(b) The select committee may only adopt rules under subsection (a0 by a unanimous vote of the voting members of the select committee.

---

**IN THE HOUSE OF REPRESENTATIVES**

**RESOLUTION**

Establishing the House Permanent Select Committee on Cybersecurity.

*Resolved,* That there is hereby established a select committee of the House to be known as the Permanent Select Committee on Cybersecurity (hereinafter referred to as the "select committee").

**SEC. 1.** (a) The select committee is authorized and directed to oversee and make continuing studies of and recommendations regarding cybersecurity threats to the United States.

(b) The select committee may report by bill or otherwise on matters within its jurisdiction.

**SEC. 2.** In this resolution:

(1) The term "cybersecurity" means the protection or defense of U.S. persons, assets, or interests in cyberspace from cyberattacks.

(2) The term "cybersecurity breach" means an attack via cyberspace, affecting an individual's or organization's use of cyberspace for the purpose of—

(A) compromising the confidentiality, availability, and/or integrity of an information system or data;

(B) disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure; or

(C) destroying the integrity of data or stealing controlled information.

(3) The term "cyberspace" means the global domain within the information environment consisting of the interdependent network of information systems infrastructures (including the Internet, telecommunications networks, computer systems, and embedded processors and controllers).

**SEC. 3.** (a) The select committee shall be composed of 21 members from the House at large, whom the Speaker and Minority Leader shall appoint in proportion to their respective control of the chamber.

(b) The Speaker and Minority Leader, and the chairpersons and ranking members of the Armed Services Committee and Select Committee on Intelligence, shall serve as ex officio, non-voting members of the select committee. As determined by the Majority Leader and Minority Leader, the chairs and ranking members of other committees deemed relevant to cybersecurity shall also be appointed as ex officio, non-voting members of the select committee.

(c) At the beginning of each Congress, the Speaker shall select a chairperson of the select committee and the Minority Leader shall select a vice chairperson for the select committee.

**SEC. 4.** The select committee may be organized into subcommittees. Each subcommittee shall have a chairperson and a vice chairperson who are selected by the chairperson and vice chairperson of the select committee, respectively.

**SEC. 5.** The select committee shall have exclusive jurisdiction and consider all proposed legislation, messages, petitions, memorials, and other matters relating to the following:

(1) Domestic and foreign cybersecurity risks (including state-sponsored threats) to the United States, including to—

(A) the computer systems of the United States;

(B) the infrastructure of the United States;

(C) citizens of the United States;

(D) corporations and other businesses in the United States; and

(E) the commerce of the United States.

(2) The development and implementation of national cybersecurity strategies and policies, including those to strengthen the digital ecosystem and improve whole-of-nation cybersecurity resilience.

(3) The activities of any department or agency relating to preventing, protecting against, or responding to cybersecurity threats to the United States, and relevant incidents or actions unless the activities, relevant incidents, or actions are conducted under authorities in title 10 or title 50, United States Code.

(4) The organization or reorganization of any department or agency to the extent that the organization or reorganization relates to a function or activity involving preventing, protecting against, or responding to cybersecurity threats to the United States, and relevant incidents or actions, unless the function or activity is conducted under authorities in title 10 or title 50, United States Code.

(5) Authorizations for appropriations, both direct and indirect, for preventing, protecting against, or responding to cybersecurity threats to the United States, and relevant incidents or actions, unless the appropriation is for functions or activities conducted under authorities in title 10 or title 50, United States Code.

**SEC. 6.** (a) The select committee is authorized in its discretion—

(1) to make investigations into any matter within its jurisdiction;

(2) to make expenditures from the contingent fund of the Senate;

(3) to employ personnel;

(4) to hold hearings;

(5) to sit and act at any time or place during the sessions, recesses, and adjourned periods of the House;

(6) to require, by subpoena or otherwise, the attendance of witnesses and the production of correspondence, books, papers, and documents;

(7) to take depositions and other testimony and authorize employees of the select committee to take depositions and other testimony;

(8) to procure the services of individual consultants, or organizations thereof, in accordance with section 202(i) of the Legislative Reorganization Act of 1946 (2 U.S.C. 4301(i));

(9) with the prior consent of the government department or agency concerned and the Committee on Rules and Administration, to use on a reimbursable basis the services of personnel of any such department or agency;

(10) to make recommendations and report legislation on matters within its jurisdiction; and

(11) to permit any personal representative of the President, designated by the President to serve as a liaison to the select committee, to attend any closed meeting of the select committee.

(b) The chairperson of the select committee or any member thereof may administer oaths to witnesses.

**SEC. 7.** (a) The select committee may only authorize issuance of a subpoena upon an affirmative vote of a majority of the members of the select committee, which vote may not be held before the time that is 48 hours after notice of the request to authorize the issuance of the subpoena is provided to each member of the select committee, absent unanimous consent.

(b) A subpoena authorized by the select committee—

(1) may be issued under the signature of the chairperson, the vice chairperson, or any member of the select committee designated by the chairperson; and

(2) may be served by any person designated by the chairperson, the vice chairperson, or other member signing the subpoena.

**SEC. 8.** The select committee shall obtain from the President and the heads of departments and agencies the information relevant to cybersecurity risks and threats required to ensure that the members of the select committee have complete and current information relating to cybersecurity activities and threats, which may include obtaining written reports reviewing—

(1) the activities carried out by the department or agency concerned to prevent, protect against, or respond to cybersecurity threats;

(2) the cybersecurity threats from within the United States and from foreign countries that are directed at the United States or its interests;

(3) previously conducted or anticipated covert actions relating to cybersecurity; and

(4) any significant cybersecurity breaches that could—

(A) affect the diplomatic, political, economic, or military relations of the United States with other countries or groups; or

(B) impose a major financial cost on the Federal government, citizens of the United States, corporations or other businesses in the United States, or the commerce of the United States.

**SEC. 9.** Each member of the select committee shall have equal and unimpeded access to information collected or otherwise obtained by the select committee.

**SEC. 10.** (a) No employee of the select committee or any person engaged by contract or otherwise to perform services for or at the request of the select committee shall be given access to any classified information by the select committee unless the employee or person has—

(1) agreed in writing and under oath to be bound by the rules of the House (including the jurisdiction of the Committee on Ethics) and of the select committee as to the security of such information during and after the period of the employment or contractual agreement with the select committee; and

(2) received an appropriate security clearance, as determined by the select committee, in consultation with the Director of National Intelligence.

(b) The type of security clearance to be required in the case of any employee or person described in subsection (a) shall, within the determination of the select committee,

in consultation with the Director of National Intelligence, be commensurate with the sensitivity of the classified information to which the employee or person will be given access by the select committee.

**SEC. 11.** (a) The head of each department and agency shall keep the select committee fully and currently informed with respect to cybersecurity activities and threats, including activities to prevent, protect against, or respond to cybersecurity threats and any significant anticipated activities relating to cybersecurity which are the responsibility of or engaged in by the department or agency.

(b) The head of any department or agency involved in any cybersecurity activities shall furnish any information or document in the possession, custody, or control of the department or agency, or person paid by the department or agency, whenever requested by the select committee with respect to any matter within the jurisdiction of the select committee.

(C) The Director of National Intelligence, the Director of the Central Intelligence Agency, the Secretary of Defense, the Secretary of Homeland Security, the Secretary of State, the Director of the Federal Bureau of Investigation, and the Secretary of Commerce shall each submit to the select committee an annual report on cyber threats.

**SEC. 12.** (a) In addition to other committee staff selected by the select committee, the select committee shall hire or appoint one employee for each member of the select committee to serve as the designated representative of the member on the select committee. The select committee shall only hire or appoint an employee chosen by a member of the select committee for whom the employee will serve as the designated representative on the select committee.

(b) The select committee shall be afforded a supplement to its budget, to be determined by the Committee on House Administration, to allow for the hire of each employee who fills the position of designated representative to the select committee. The designated representative shall have office space and appropriate office equipment in the select committee spaces. Designated personal representatives shall have the same access to committee staff, information, records, and databases as select committee staff, as determined by the chairperson and vice chairperson.

(C) Each designated employee, as authorized by subsection (a), shall meet all the requirements of relevant statutes, House rules, and committee security clearance requirements for employment by the select committee.

(d) Of the amounts made available to the select committee for personnel—

(1) not more than 60 percent shall be under the control of the chairperson; and

(2) not less than 40 percent shall be under the control of the vice chairperson.

**SEC. 13.** (a) The select committee shall adopt rules (not inconsistent with the rules of the House and in accordance with rule XI of the Standing Rules of the House) governing the procedure of the select committee, which shall include addressing how often the select committee shall meet, meeting times and location, type of notifications, notices of hearings, duration of the select committee, and records of the select committee after committee activities are complete.

(b) The select committee may only adopt rules under subsection (a) by a unanimous vote of the voting members of the select committee.

## 1.3 Establish a National Cyber Director (NCD)

Congress should establish a National Cyber Director (NCD), within the Executive Office of the President, who is Senate-confirmed and supported by an "Office of the National Cyber Director". The NCD would serve as the President's principal advisor for cybersecurity and associated emerging technology issues; the lead for national-level coordination for cyber strategy, policy, and defensive cyber operations; and the chief U.S. representative and spokesperson on cybersecurity issues.

---

**A BILL**

To establish a National Cyber Director within the Executive Office of the President in order to improve national-level coordination for cyber strategy, policy, and defensive cyber operations, and for other purposes.

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

**SEC. 1. NATIONAL CYBER DIRECTOR.**

The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

(1) by inserting after section 2214 the following new section:

**"SEC. 2215. National Cyber Director**

"(a) ESTABLISHMENT WITHIN THE EXECUTIVE OFFICE OF THE PRESIDENT.—There is established within the Executive Office of the President the Office of the National Cyber Director (hereinafter in this section referred to as the "Office").

"(b) NATIONAL CYBER DIRECTOR.—

"(1) The Office shall be headed by the National Cyber Director (hereinafter in this section referred to as the "Director") who shall be appointed by the President, by and with the advice and consent of the Senate. As an exercise of the rulemaking power of the Senate, any nomination of the National Cyber Director submitted to the Senate for confirmation, and referred to a committee, shall be jointly referred to the Senate Homeland Security and Governmental Affairs Committee and the Senate Armed Services Committee. The National Cyber Director shall hold office at the pleasure of the President, and shall be entitled to receive the same pay and allowances as are provided in 5 U.S.C. 5314, under Level I of the Executive Schedule.

"(2) There shall be two Deputy National Cyber Directors, who shall be appointed by the President, shall hold office at the pleasure of the President, shall report to the National Cyber Director, and may hold positions in departments and agencies of the Federal Government—

"(A) The Deputy National Cyber Director for Strategy, Capabilities, and Budget; and

"(B) The Deputy National Cyber Director for Plans and Operations.

"(c) RESPONSIBILITIES OF THE DIRECTOR.—

"(1) IN GENERAL—The Director shall, subject to the authority, direction, and control of the President—

"(A) serve as the principal advisor to the President on cybersecurity strategy and policy and associated emerging technology issues;

"(B) develop and, upon approval of the President, supervise the implementation of, in consultation with appropriate Federal departments and agencies, the United States' National Cyber Strategy, including—

"(i) in consultation with the Director of the Office of Management and Budget, monitoring and assessing the effectiveness of Federal departments and agencies' implementation of the strategy;

"(ii) making recommendations relevant to changes in the organization, personnel and resource allocation, and policies to the Director of the Office of Management and Budget and heads of Federal departments and agencies in order to implement the strategy;

"(iii) reviewing the annual budget proposal for each Federal department or agency and certifying to the head of each Federal department or agency and the Director of the Office Management and Budget whether the department or agency proposal is consistent with the National Cyber Strategy;

"(iv) continuously assessing and making relevant recommendations to the President on the appropriate level

of integration and interoperability across the Federal cybersecurity operations centers;

"(v) as a part of the strategy, coordinating with the Federal Chief Information Officer and the Federal Chief Information Security Officer to streamline Federal regulations, policies, and guidelines related to issues of cybersecurity; and

"(vi) reporting annually to the President and the Congress on the state of U.S. cybersecurity, the effectiveness of the National Cybersecurity Strategy, and the status of Federal departments and agencies implementation of the strategy;

"(C) lead joint interagency planning for the Federal Government's integrated response to cyberattacks and cyber campaigns of significant consequence, to include—

"(i) coordinating with relevant Federal departments and agencies in the development of, for the approval of the President, joint, integrated operational plans, processes, and playbooks for incident response that—

"(I) feature clear lines of authority and lines of effort across the Federal Government;

"(II) feature authorities that have been delegated to an appropriate level to facilitate effective operational responses across the Federal Government;

"(III) reflect integration of defensive cyber plans and capabilities with offensive cyber plans and capabilities; and

"(IV) reflect integration and understanding of private sector and State, local, territorial, and tribal capabilities and requirements;

"(ii) exercising these operational plans, processes, and playbooks; and

"(iii) coordinating these operational plans, processes, and playbooks for incident response with ongoing offensive cyber plans and operations; and

"(iv) ensuring these plans, processes, and playbooks are properly coordinated with relevant private sector entities, as appropriate.

"(D) direct the Federal Government's response to cyberattacks and cyber campaigns of significant consequence, to include—

"(i) developing for the approval of the President, with the heads of relevant departments and agencies independently or through the National Security Council as directed by the President, operational priorities, requirements, and tasks;

"(ii) coordinating, deconflicting, and directing the execution of operational activities in incident response; and

"(iii) coordinating operational activities with relevant private sector entities.

"(E) serve as the focal point for private sector leaders to engage the executive branch on cybersecurity and emerging technology issues with the support of, and in coordination with, the Cybersecurity and Infrastructure Security Agency; and

"(F) annually report to Congress, in a closed or public setting, on cybersecurity threats and issues facing the nation, including any new or emerging technologies that may impact national security, economic prosperity, or enforcing the rule of law; and

"(G) be responsible for such other functions as the President may direct.

"(2) ADDITIONAL AUTHORITIES.—At the discretion of the President, the Director may—

"(A) serve as the senior representative on any body that the President may establish for the purpose of providing to the President advice on cybersecurity;

"(B) be empowered to convene National Security Council, National Economic Council, and Homeland Security Council meetings, with the concurrence of the National Security Advisor, Homeland Security Advisor, or Director of the National Economic Council, as appropriate;

"(C) be included as a participant in preparations for and, if appropriate, execution of all cybersecurity summits and other international meetings at which cybersecurity is a major topic;

"(D) delegate any of the Director's functions, powers, and duties to such officers and employees of the Office as he may designate; and

"(E) authorize such successive re-delegations of such functions, powers, and duties to such officers and employees of the Office as he may deem appropriate.

"(3) ATTENDANCE AND PARTICIPATION IN MEETING OF NATIONAL SECURITY COUNCIL.—Section 101(c)(2) of the National Security Act of 1947 (50 U.S.C. 3021(c)(2)) is amended by striking "and the Chairman of the Joint Chiefs of Staff" and inserting "the Chairman of the Joint Chiefs of Staff, and the National Cyber Director."

"(4) AUTHORITIES OF THE DIRECTOR.—The Director may, for the purpose of carrying out the Director's functions under this section—

"(A) subject to the civil service and classification laws, select, appoint, employ, and fix the compensation of such officers and employees as are necessary and prescribe their authority and duties, except that not more than 100 individuals may be employed without regard to any provision of law regulating the employment or compensation at rates not to exceed the rate of pay for level IV of the Executive Schedule in section 5314 [5315] of title 5, United States Code;

"(B) employ experts and consultants in accordance with section 3109 of title 5, United States Code, and compensate individuals so employed for each day (including travel time) at rates not in excess of the maximum rate of pay for grade GS-15 as provided in section 5332 of title 5, United States Code, and while such experts and consultants are so serving away from their homes or regular place of business, to pay such employees travel expenses and per diem in lieu of subsistence at rates authorized by section 5703 of title 5, United States Code, for persons in Government service employed intermittently;

"(C) promulgate such rules and regulations as may be necessary to carry out the functions, powers and duties vested in the Director;

"(D) utilize the services, personnel, and facilities of Federal departments and agencies with the consent of the heads of such departments and agencies;

"(E) enter into and perform such contracts, leases, cooperative agreements, or other transactions as may be necessary in the conduct of the work of the Office and on such terms as the Director may deem appropriate, with any agency or instrumentality of the United States, or with any public or private person, firm, association, corporation, or institution;

"(F) accept voluntary and uncompensated services, notwithstanding the provisions of section 1342 of title 31, United States Code;

"(G) adopt an official seal, which shall be judicially noticed; and

"(H) provide, where authorized by law, copies of documents to persons at cost, except that any funds so received shall be credited to, and be available for use from, the account from which expenditures relating thereto were made.

(2) in the table of contents, by inserting after the item relating to section 2214 the following new item:

"Sec. 2215. National Cyber Director."

# 1.4.a Strengthen the Cybersecurity and Infrastructure Security Agency (CISA)

This proposal implements the Commission's recommendation to strengthen the Cybersecurity and Infrastructure Security Agency (CISA) by extending the term limit of the Director of the Agency to five years and to develop a report and recommendations to Congress on how to bolster the Cybersecurity and Infrastructure Security Agency's resources, whether CISA's facilities are adequate, and the authorities needed to perform threat hunting across the .gov domain.

---

## A BILL

To strengthen the Cybersecurity and Infrastructure Security Agency, and for other purposes.

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

### SEC. 1. CISA DIRECTOR TERM APPOINTMENT.

(a) IN GENERAL.—Paragraph (b)(1) of section 2202 of the Homeland Security Act of 2002 (6 U.S.C. 652), is amended by inserting "Each Director shall serve for a term of five 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 confirmation of a new Director of the Cybersecurity and Infrastructure Protection Agency of the Department of Homeland Security, or

(2) January 1, 2021.

(c) TITLE V.—Subchapter II of Chapter 53 of title 5, United States Code, is amended—

(1) in section 5313, by inserting "Director, Cybersecurity and Infrastructure Security Agency." after "Administrator of the Transportation Security Administration."; and

(2) in section 5314, by striking "Director, Cybersecurity and Infrastructure Security Agency.".

SEC. 2. AGENCY REVIEW.

(a) REQUIREMENT OF COMPREHENSIVE REVIEW.—In order to strengthen the Cybersecurity and Infrastructure Security Agency within the Department of Homeland Security, the Secretary of Homeland Security shall conduct a comprehensive review of the ability of the Cybersecurity and Infrastructure Security Agency to fulfill its current missions, as well as the recommendations detailed in the U.S. Cyberspace Solarium Commission's Report.

(b) ELEMENTS OF REVIEW.—The review conducted under subsection (a) shall include the following elements:

(1) An assessment of how additional budget resources could be used by the Cybersecurity and Infrastructure Security Agency for projects and programs that—

(A) support the national risk management mission;

(B) support public and private-sector cybersecurity;

(C) promote public-private integration; and

(D) provide situational awareness of cybersecurity threats.

(2) A comprehensive force structure assessment of the Cybersecurity and Infrastructure Security Agency including—

(A) a determination of the appropriate size and composition of personnel to accomplish the mission of the Agency, as well as the recommendations detailed in the U.S. Cyberspace Solarium Commission's Report;

(B) an assessment of whether existing personnel are appropriately matched to the prioritization of threats in the cyber domain and risks in critical infrastructure;

(C) an assessment of whether the Agency has the appropriate personnel and resources to—

(i) perform risk assessments, threat hunting, incident response to support both private and public cybersecurity;

(ii) carry out its responsibilities related to the security of Federal information and Federal information systems;

(iii) carry out its critical infrastructure responsibilities, including national risk management;

(D) an assessment of whether current structure, personnel, and resources of regional field offices are sufficient in fulfilling agency responsibilities and mission requirements.

(c) SUBMISSION OF REVIEW.—Not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security shall submit a report to Congress detailing the result of the assessments required by subsection (b), including recommendations to address any identified gaps.

## SEC. 3. GENERAL SERVICES ADMINISTRATION REVIEW.

(a) REVIEW. —The Administrator of the General Services Administration shall—

(1) conduct a review of current Cybersecurity and Infrastructure Security Agency facilities and assess their suitability to fully support current and projected mission requirements nationally and regionally; and

(2) make recommendations regarding resources needed to procure or build a new facility or augment existing facilities to ensure sufficient size and accommodations to fully support current and projected mission requirements, including the integration of personnel from the private sector and other departments and agencies.

(b) SUBMISSION OF REVIEW.—Not later than one year after the date of the enactment of this Act, the Administrator shall submit the review required by subsection (a) to the President, the Secretary of Homeland Security, and to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives.

## 1.4.b Establish Authority for CISA to Threat Hunt on the .gov Domain

This proposal implements the Commission's recommendation to strengthen the Cybersecurity and Infrastructure Security Agency by granting it authorities needed to perform threat hunting across the .gov domain.

---

**A BILL**

To authorize the Cybersecurity and Infrastructure Security Agency to perform threat hunting identification on Federal networks, and for other purposes.

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

**SEC. 1. THREAT HUNTING IDENTIFICATION ON FEDERAL NETWORKS.**

(a) AUTHORITY.—Subsection (b) of section 3553 of title 44, United States Code, is amended—

(1) in paragraph (6), by striking "; and" and inserting ";";

(2) by redesignating paragraph (7) as paragraph (8); and

(3) by inserting the following new paragraph (7):

"(7) hunting for and identifying, with or without advance notice, threats and vulnerabilities within Federal information systems; and".

(b) BINDING OPERATIONAL DIRECTIVE.—Not later than one year following the enactment of this section, the Secretary of Homeland Security shall issue a binding operational directive pursuant to subsection (b)(2) of section 3553 of title 44, United States Code, to implement the authority provided in subsection (a).

## 1.4.1 Codify and Strengthen the Cyber Threat Intelligence Integration Center (CTIIC)

This proposal implements the Commission's recommendation to codify the Cyber Threat Intelligence Integration Center (CTIIC) through legislation, using as a model the 2015 Presidential Memorandum that created the center, and strengthen CTIIC's ability to carry out its responsibilities, especially in enhancing the quality and speed of attribution.

---

**A BILL**

To codify and strengthen the Cyber Threat Intelligence Integration Center with a focus on enhancing the quality and speed of attribution, and for other purposes.

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

**SEC. 1. ESTABLISHMENT OF THE CYBER THREAT INTELLIGENCE INTEGRATION CENTER.**

(a) ESTABLISHMENT OF CENTER.—There is established within the Office of the Director of National Intelligence a Cyber Threat Intelligence Integration Center.

(b) DIRECTOR OF CYBER THREAT INTELLIGENCE INTEGRATION CENTER.—The Cyber Threat Intelligence Integration Center shall be headed by a Director of Cyber Threat Intelligence Integration, who—

(1) shall report to the Director of National Intelligence; and

(2) may not simultaneously serve in any other capacity in the executive branch.

(c) PRIMARY MISSIONS OF THE CENTER.—The primary missions of the Cyber Threat Intelligence Integration Center shall be as follows:

(1) Provide integrated all-source analysis of intelligence related to foreign cyber threats or related to cyber incidents affecting U.S. national interests.

(2) Support the National Cybersecurity and Communications Integration Center, the National Cyber Investigative Joint Task Force, U.S. Cyber Command, and other relevant United States Government entities by providing access to intelligence necessary to carry out their respective missions.

(3) Oversee the development and implementation of intelligence sharing capabilities (including systems, programs, policies, and standards) to enhance shared situational awareness of intelligence related to foreign cyber threats or related to cyber incidents affecting U.S. national interests among the organizations referenced in subsection (b) of this section.

(4) Ensure that indicators of malicious cyber activity and, as appropriate, related threat reporting contained in intelligence channels are downgraded to the lowest classification practicable for distribution to both United States Government and U.S. private sector entities through the mechanism described in section 4 of Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity).

(5) Facilitate and support interagency efforts to develop and implement coordinated plans to counter foreign cyber threats to U.S. national interests using all instruments of national power, including diplomatic, economic, military, intelligence, homeland security, and law enforcement activities.

(6) Serve as the lead coordinator for the U.S. Intelligence Community's analytic assessment for cyber attribution and as the central and shared knowledge bank on cyber actors, as well as their goals, strategies, capabilities, and sponsoring organizations.

## 1.5 Recruit, Develop, and Retain a Stronger Federal Cyber Workforce

This proposal implements the recommendation to recruit, develop, and retain a stronger Federal cyber workforce by clarifying strategy and coordination of cyber workforce development efforts throughout the government and authorizing systems and tools needed for implementation. Specifically, the proposal implements eight elements of the Commission's Federal cyber workforce recommendation:

- Reinforce and authorize the role of the National Initiative for Cybersecurity Education (NICE) in coordinating U.S. government efforts to advance cybersecurity workforce development nationwide, and resource the office sufficiently for this role.

- Expand the existing CyberCorps: Scholarship for Service program.

- Expand cybersecurity programs in the National Science Foundation, and promote research into the current state of the cyber workforce, paths to entry, and demographics.

- Direct the Office of Personnel Management (OPM), in partnership with Federal departments and agencies including the National Institute for Science and Technology (NIST) and Department of Homeland Security (DHS), to create a distinct cyber occupational series and provide a report evaluating the potential for a new Cyber Civil Service: a system of established cyber career paths that allows movement between departments and agencies and into senior leadership positions.

- Direct and fund the Cybersecurity and Infrastructure Security Agency (CISA) to design a process for one- to three-year exchange assignments of cyber experts between CISA and the private sector.

- Direct the Department of Veterans Affairs, OPM, NICE, and Department of Defense (DoD) to design cybersecurity-specific upskilling and transition assistance programs for veterans and transitioning military service members to move into Federal civilian cybersecurity jobs.

- Examine the impact of Security Clearance processing times on workforce development and retention, and establish expedited security clearance process for DoD Cyber Excepted Service personnel.

- Require appropriate departments and agencies to develop training for managers to cultivate practices that foster a more diverse cyber workforce and more inclusive work environment.

---

**A BILL**

To improve the cyber workforce of the United States, and for other purposes.

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

## SEC. 1. SHORT TITLE.

This Act may be cited as the "Creating a Consolidated Federal Strategy and Tools for the Cyber Workforce Act of 2020" or the "Cyber Workforce Act of 2020".

## SEC. 2. IMPROVING NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

(a) PROGRAM IMPROVEMENTS GENERALLY.—Subsection (a) of section 401 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7451) is amended—

(1) in paragraph (5), by striking "; and" and inserting a semicolon;

(2) by redesignating paragraph (6) as paragraph (9); and

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

"(6) identifying cybersecurity workforce skill gaps in public and private sectors;

"(7) advancing the cybersecurity education and training of the Federal workforce by facilitating coordination of Federal programs, including—

"(A) the GenCyber Program of the National Security Agency and the National Science Foundation;

"(B) the National Centers of Academic Excellence in Cybersecurity program of the National Security Agency and the Department of Homeland Security;

"(C) the Federal Cyber Scholarship for Service program of the National Science Foundation;

"(D) the apprenticeship program of the Department of Labor;

"(E) the Cybersecurity Education and Training Assistance Program of the Department of Homeland Security; and

"(F) such other programs as the Director considers appropriate;

"(8) developing metrics to measure the effectiveness and effect of programs and initiatives to advance the cybersecurity workforce; and".

(b) STRATEGIC PLAN.—Subsection (c) of section 401 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7451) is amended—

(1) by striking "The Director" and inserting the following:

"(1) IN GENERAL.—The Director"; and

(2) by adding at the end the following:

"(2) REQUIREMENT.—The strategic plan developed and implemented under paragraph (1) shall include a description of how the Director will implement this section.".

(c) CYBERSECURITY CAREER PATHWAYS.—

(1) IDENTIFICATION OF MULTIPLE CYBERSECURITY CAREER PATHWAYS.—In carrying out subsection (a) of section 401 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7451) and not later than one year after the date of the enactment of this Act, the Director shall consult with other Federal agencies, academia, and industry to identify multiple career pathways for cybersecurity work roles that can be used in the private and public sectors.

(2) REQUIREMENTS.—The Director shall ensure that the multiple cybersecurity career pathways identified under paragraph (1) indicate the knowledge, skills, and abilities, including relevant education, training, apprenticeships, certifications, and other experiences, that—

(A) align with employers' cybersecurity skill needs, including proficiency level requirements, for its workforce; and

(B) prepare an individual to be successful in entering or advancing in a cybersecurity career.

(3) FEDERAL CAREERS.—The Director, in coordination with the Director of the Office of Personnel Management, shall identify career opportunities in the Federal government for the cybersecurity career pathways identified under paragraph (1), including noncompetitive hiring pathways, including for individuals who participate in Federal cybersecurity workforce training programs referred to in section 401(a)(7) of the Cybersecurity Enhancement Act of 2014, as added by subsection (a)(3).

(d) PROFICIENCY TO PERFORM CYBERSECURITY TASKS.—Not later than one year after the date of the enactment of this Act, the Director shall—

(1) in carrying out subsection (a) of section 401 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7451), assess the scope and sufficiency of efforts to measure a learner's capability to perform specific tasks found in the National Initiative for Cybersecurity Education (NICE) Cybersecurity

Workforce Framework (NIST Special Publication 800–181) at all proficiency levels; and

(2) submit to Congress a report—

(A) on the findings of the Director with respect to the assessment carried out under paragraph (1); and

(B) with recommendations for effective methods for measuring the cybersecurity proficiency of learners.

(e) CYBERSECURITY METRICS.—Such section is further amended by adding at the end the following:

"(e) CYBERSECURITY METRICS.—In carrying out subsection (a), the Director, in coordination with such agencies as the Director considers relevant, shall develop repeatable measures and reliable metrics for measuring and evaluating Federally funded cybersecurity workforce programs and initiatives based on the outcomes of such programs and initiatives."

(f) TRANSFER AND REPEAL.—The Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7451), as amended by this section, is further amended—

(1) by redesignating section 401 as section 303 and transferring section 303, as so redesignated, to the end of title III of such Act;

(2) by striking title IV in its entirety; and

(3) in the table of contents, by—

(A) striking the items relating to title IV and section 401; and

(B) inserting after the item relating to section 302 the following:

**"Sec. 303. National cybersecurity awareness and education program.".**

(g) CONFORMING AMENDMENTS.—

(1) Section 302(3) of the Federal Cybersecurity Workforce Assessment Act of 2015 (Public Law 114–113) is amended by striking "under section 401 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7451)" and inserting "under section 303 of the Cybersecurity Enhancement Act of 2014 (Public Law 113–274)".

(2) Section 2(c)(3) of the NIST Small Business Cybersecurity Act (Public Law 115–236) is amended by striking "under section 401 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7451)" and inserting "under section 303 of the Cybersecurity Enhancement Act of 2014 (Public Law 113–274)".

(3) Section 302(f) of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7442(f)) is amended by striking "under section 401" and inserting "under section 303".

**SEC. 3. MODIFICATIONS TO FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.**

Section 302 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7442) is amended—

(1) in subsection (b)—

(A) in paragraph (2), by striking "information technology" and inserting "information technology and cybersecurity";

(B) by amending paragraph (3) to read as follows:

"(3) prioritize the placement of scholarship recipients fulfilling the post-award employment obligation under this section to ensure that—

"(A) not less than 70 percent of such recipients are placed in an executive agency (as defined in section 105 of title 5, United States Code);

"(B) not more than ten percent of such recipients are placed as educators in the field of cybersecurity at qualified institutions of higher education that provide scholarships under this section; and

"(C) not more than 20 percent of such recipients are placed in positions described in paragraphs (2) through (5) of subsection (d); and"; and

(C) in paragraph (4), in the matter preceding subparagraph (A), by inserting ", including by seeking to provide awards in coordination with other relevant agencies for summer cybersecurity camp or other experiences, including teacher training, in each of the 50 States," after "cybersecurity education";

(2) in subsection (d)—

(A) in paragraph (4), by striking "or" at the end;

(B) in paragraph (5), by striking the period at the end and inserting "; or"; and

(C) by adding at the end the following:

"(6) as provided by subsection (b)(3)(B), a qualified institution of higher education."; and

(3) in subsection (m)—

(A) in paragraph (1), in the matter preceding subparagraph (A), by striking "cyber" and inserting "cybersecurity"; and

(B) in paragraph (2), by striking "cyber" and inserting "cybersecurity".

**SEC. 4. CYBERSECURITY IN PROGRAMS OF THE NATIONAL SCIENCE FOUNDATION.**

(a) COMPUTER SCIENCE AND CYBERSECURITY EDUCATION RESEARCH.—Section 310 of the American Innovation and Competitiveness Act (42 U.S.C. 1862s–7) is amended—

(1) in subsection (b)—

(A) in paragraph (1), by inserting "and cybersecurity" after "computer science"; and

(B) in paragraph (2)—

(i) in subparagraph (C), by striking "; and" and inserting a semicolon;

(ii) in subparagraph (D), by striking the period at the end and inserting "; and"; and

(iii) by adding at the end the following:

"(E) tools and models for the integration of cybersecurity and other interdisciplinary efforts into computer science education and computational thinking at secondary and postsecondary levels of education."; and

(2) in subsection (c), by inserting ", cybersecurity," after "computing".

(b) SCIENTIFIC AND TECHNICAL EDUCATION.—Section 3(j)(9) of the Scientific and Advanced-Technology Act of 1992 (42 U.S.C. 1862i(j)(9)) is amended by inserting "and cybersecurity" after "computer science".

(c) LOW-INCOME SCHOLARSHIP PROGRAM.—Section 414(d) of the American Competitiveness and Workforce Improvement Act of 1998 (42 U.S.C. 1869c) is amended—

(1) in paragraph (1), by striking "or computer science" and inserting "computer science, or cybersecurity"; and

(2) in paragraph (2)(A)(iii), by inserting "cybersecurity," after "computer science,".

(d) SCHOLARSHIPS AND GRADUATE FELLOWSHIPS.—The Director of the National Science Foundation shall ensure that students pursuing master's degrees and doctoral degrees in fields relating to cybersecurity are considered as applicants for scholarships and graduate fellowships under the Graduate Research Fellowship Program under section 10 of the National Science Foundation Act of 1950 (42 U.S.C. 1869).

(e) PRESIDENTIAL AWARDS FOR TEACHING EXCELLENCE.—The Director of the National Science Foundation shall ensure that educators and mentors in fields relating to cybersecurity can be considered for—

(1) Presidential Awards for Excellence in Mathematics and Science Teaching made under section 117 of the National Science Foundation Authorization Act of 1988 (42 U.S.C. 1881b); and

(2) Presidential Awards for Excellence in STEM mentoring administered under section 307 of the American Innovation and Competitiveness Act (42 U.S.C. 1862s–6).

(f) CYBER WORKFORCE DEVELOPMENT RESEARCH PROGRAM.—

(1) IN GENERAL.—The Director of the National Science Foundation shall carry out a basic research program on the cyber workforce, including the competitive award of grants to institutions of higher education or eligible nonprofit organizations (or consortia thereof).

(2) RESEARCH.—In carrying out research and awarding grants pursuant to paragraph (1), the Director of the National Science Foundation shall support basic research on the current state of the cyber workforce, paths to entry,

demographic trends of the cyber workforce, and other closely related topics as the director determines appropriate.

(3) REQUIREMENTS.—In carrying out the activities described in paragraph (1), the Director of the National Science Foundation shall—

(A) use the existing programs and prior research of the National Science Foundation, in collaboration with the National Institute for Standards and Technology, including the National Initiative for Cybersecurity Education, the Department of Homeland Security, the Department of Defense, the Office of Personnel Management, and other Federal departments and agencies, as appropriate;

(B) align with or build on the National Initiative on Cybersecurity Education Cybersecurity Workforce Framework wherever practicable and applicable;

(C) leverage the collective body of knowledge from existing cyber workforce development research and education activities; and

(D) engage with other Federal departments and agencies, research communities, and potential users of information produced under this section.

**SEC. 5. CONNECTING AND ENABLING INTERAGENCY MANEUVERABILITY OF THE FEDERAL CYBER WORKFORCE.**

(a) CYBER OCCUPATIONAL SERIES.—Not later than one year after the date of enactment of this Act, the Director of the Office of Personnel Management, in coordination with Federal departments and agencies, including the National Institute of Standards and Technology, the Department of Homeland Security, and the Department of Defense, shall create an occupational series specific to Federal cyber positions that—

(1) aligns with the Cybersecurity Workforce Framework published by the National Institute of Standards and Technology in Special Publication 800-181 to the greatest extent practicable, but is not required to include every work role included in the Framework; and

(2) may include roles outside the Framework if necessary.

(b) PLAN REQUIRED.—Not later than one year after the date of enactment of this Act, the Director of the Office of Personnel Management, in coordination with Federal departments and agencies including the National Institute of Standards and Technology and the Department of Homeland Security 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 strategic plan to build a flexible and connected cohort among Federal civil service cyber workers, and an office responsible for executing the strategy.

(c) ELEMENTS.—The plan required under subsection (b) shall include the following:

(1) A system of established cyber career paths that allows movement between departments and agencies and into senior leadership positions that would inform the activities of the office described in (b).

(2) A standardized system for evaluating worker knowledge, skills, and abilities in the workforce that provides demonstrated equivalences in work across the government, aligned to the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework.

(3) A strategy for implementing the lessons learned and best practices in cyber talent management from across the Federal government.

(4) A strategy for building greater connectivity and opportunities for interaction between members of the Federal cyber workforce.

(5) A system for counting occurrences of cyber candidates in the Federal application and hiring process who have chosen to leave the application or hiring process. The system shall—

(A) anonymize individuals' data;

(B) provide these individuals with a means for communicating their reasons for leaving the hiring process; and

(C) to the greatest extent practicable make this data available for public review, exclusive of data reported from intelligence agencies.

(6) A review of competitions and challenges carried out under section 301 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7441) and their effectiveness in identifying, developing, and recruiting talented individuals to perform duties relating to the security of information technology in Federal, State, local, and tribal government agencies.

(7) An assessment of options and recommendation for organizational placement and leadership structure for the office described in (b).

(8) A timeline for the establishment of the office described in (b).

(d) FORM OF PLAN.—The plan required under subsection (b) shall be submitted in unclassified form, but may include a classified annex.

## SEC. 6. ESTABLISHING A PUBLIC-PRIVATE TALENT EXCHANGE FOR CYBERSECURITY SKILLS DEVELOPMENT.

(a) PURPOSE.—There is established, within the Cybersecurity and Infrastructure Security Agency, a pilot program for the purpose of carrying out a talent exchange program between the private sector and the Federal government in order to—

(1) Facilitate close collaboration with the best and most diverse minds from outside the government to improve national security;

(2) Incorporate public and private sector talent to challenge thinking, test innovative ideas and enable greater understanding on cyber security, bringing industry and government expertise together in a way that helps both institutions learn lessons, identify systemic vulnerabilities and reduce the future impact of cyberattacks, and

(3) Expand existing Cybersecurity and Infrastructure Security Agency programs that integrate private sector and interagency personnel.

(b) REQUIREMENTS.—In carrying out the public-private talent exchange established pursuant to subsection (a), the Director of the Cybersecurity and Infrastructure Security Agency shall—

(1) Promote public-private cooperation and intelligence sharing;

(2) Develop and publicize the knowledge, skills, and abilities, including relevant education, training, apprenticeships, certifications, and other experiences, that are required to participate in the program;

(3) Provide for participation by cleared and uncleared public and private employees; and

(4) Develop a plan and application process for the private sector.

(c) ASSIGNMENT AUTHORITY.— Under regulations prescribed by the Secretary of Homeland Security to carry out this section, the Director of the Cybersecurity and Infrastructure Security Agency may, with the agreement of a private-sector organization and the consent of the employee, arrange for the temporary assignment of an employee to such private-sector organization, or from such private-sector organization to a Cybersecurity and Infrastructure Security Agency organization under this section.

(d) AGREEMENTS.—

(1) IN GENERAL.— Prior to any temporary assignment pursuant to the authority provided in subsection (c), the Director of the Cybersecurity and Infrastructure Security Agency shall enter into a written agreement with, the private-sector organization and the employee concerned regarding the terms and conditions of the employee's assignment under this section. The agreement shall—

(A) require that the employee of the Cybersecurity and Infrastructure Security Agency, upon completion of the assignment, will serve in the Cybersecurity and Infrastructure Security Agency, or elsewhere in the civil service, if approved by the Director, for a period of time equal to twice the length of the assignment;

(B) provide that if the employee of the Cybersecurity and Infrastructure Security Agency or of the private-sector organization (as the case may be) fails to carry out the agreement, such employee shall be liable to the United States for payment of all expenses of the assignment, including, but not limited to, the value of the employee's salary and benefits, unless that failure was for good cause as determined by the Director; and

(C) contain language prohibiting an employee of the Cybersecurity and Infrastructure Security Agency from improperly utilizing pre-decisional or draft deliberative information that such employee may be privy to or aware of related to Department programing, budgeting, resourcing, acquisition, or procurement for the benefit or advantage of the private-sector organization.

(2) COLLECTION OF COSTS.—

(A) In general.—An amount for which an employee is liable under paragraph (1)(B) shall be treated as a debt due the United States.

(B) Waiver.—The Director may waive, in whole or in part, collection of a debt described in subparagraph (A) based on a determination that the collection would be against equity and good conscience and not in the best interests of the United States, after taking into account any indication of fraud, misrepresentation, fault, or lack of good faith on the part of the employee.

(e) TERMINATION.— An assignment under this section may, at any time and for any reason, be terminated by the Cybersecurity and Infrastructure Security Agency or the private-sector organization concerned.

(f) DURATION.— An assignment under this section shall be for a period of not less than one year and not more than three years. No employee of the Cybersecurity and Infrastructure Security Agency may be assigned under this section for more than a total of 4 years inclusive of all such assignments.

(g) STATUS OF FEDERAL EMPLOYEES ASSIGNED TO PRIVATE-SECTOR ORGANIZATIONS.— An employee of the Cybersecurity and Infrastructure Security Agency who is assigned to a private-sector organization under this section shall be considered, during the period of assignment, to be employed by the Agency for all purposes. The written agreement entered into pursuant to subsection (d)(1) shall address the specific terms and conditions related to the employee's continued status as a Federal employee.

(h) MISSION CONTINUITY.—Prior to authorizing the temporary assignment of an employee of the Cybersecurity and Infrastructure Security Agency to a private-sector organization, the Director of the Cybersecurity and Infrastructure Security Agency shall—

(1) ensure that the normal duties and functions of such employee can be reasonably performed by other employees of the Cybersecurity and Infrastructure Security Agency without the permanent transfer or reassignment of other personnel of the Cybersecurity and Infrastructure Security Agency;

(2) ensure that the normal duties and functions of such employees are not, as a result of and during the course of such temporary assignment, performed or augmented by contractor personnel in violation of the provisions of section 1710 of Title 41; and

(3) certify that the temporary assignment of such employee shall not have an adverse or negative impact on mission attainment or organizational capabilities associated with the assignment.

(i) TERMS AND CONDITIONS FOR PRIVATE-SECTOR EMPLOYEES.—An employee of a private-sector organization who is assigned to a Cybersecurity and Infrastructure Security Agency organization under this section—

(1) shall continue to receive pay and benefits from the private-sector organization from which such employee is assigned and shall not receive pay or benefits from the Cybersecurity and Infrastructure Security Agency;

(2) may be placed in roles onsite at CISA, or in other non-embedded positions.

(3) shall not have access to any trade secrets or to any other nonpublic information which is of commercial value to the private-sector organization from which such employee is assigned;

(4) may perform work that is considered inherently governmental in nature only when requested in writing by the Director of the Cybersecurity and Infrastructure Security Agency; and

(5) may not be used to circumvent the provision of section 1710 of title 41, United States Code, nor to circumvent any limitation or restriction on the size of Cybersecurity and Infrastructure Security Agency's workforce.

(j) PROHIBITION AGAINST CHARGING CERTAIN COSTS TO THE FEDERAL GOVERNMENT.—A private-sector organization may not charge Cybersecurity and Infrastructure Security Agency, or any other agency of the Federal government, as direct or indirect costs under a Federal contract, the costs of pay or benefits paid by the organization to an employee on a temporary assignment pursuant to this section.

(k) CONFLICTS OF INTEREST.—A private-sector organization that is temporarily assigned a member of the Cybersecurity and Infrastructure Security Agency workforce under this section shall not be considered to have a conflict of interest with the Department of Homeland Security solely because of participation in the program established under this section.

(l) REPORTING REQUIREMENT.—The Director of the Cybersecurity and Infrastructure Security Agency shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives, not later than one month after the end of the fiscal year involved, a report on any activities carried out utilizing the authorities provided by this section during such fiscal year, including information concerning—

(1) the private-sector organizations to and from which any employee was assigned under this section;

(2) the positions those employees held while they were so assigned;

(3) a description of the tasks they performed while they were so assigned; and

(4) a discussion of any actions that might be taken to improve the effectiveness of the program under this section, including any proposed changes in law.

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

(1) Value is derived from the exchange program described in this section when participants are meaningfully integrated into their host organizations, which will often require a personnel security clearance process for participants from the private sector.

(2) The success of the program described in this section, and the workforce development efforts critical for the success of key national security priorities more generally, are severely hampered by the current personnel security clearance process.

(3) Until such time as the wait times for personnel security clearances meet the stated goals of Federal departments and agencies, in order to implement the program described in subsection (a), the Director of the Cybersecurity and Critical Infrastructure Agency should encourage—

(A) declassification of information as broadly and quickly as practicable; and

(B) participation of the private sector at the unclassified level to promote open dialogue and information sharing, outside the classified space.

## SEC. 7. VETERANS UPSKILLING PROGRAM FOR CYBER WORKFORCE

(a) IN GENERAL.—The Secretary of Veterans Affairs ("the Secretary") shall, not later than one year after the date of enactment of this Act, establish a pilot program under which the Secretary shall provide cybersecurity-specific upskilling for veterans and transitioning military service members, which incorporates—

(1) virtual platforms for coursework and training;

(2) work-based learning opportunities and programs;

(3) alignment with the taxonomy, knowledge, skills, abilities, and tasks from the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST Special Publication 800–181), or successor framework; and

(4) portable credentials.

(b) COORDINATION.—In the development of the pilot program described in subsection (a), the Secretary shall coordinate with the Director of the National Institute of Standards and Technology, the Secretary of Homeland Security, the Secretary of Defense, the Secretary of Labor, and the Director of the Office of Personnel Management to leverage existing platforms and frameworks for providing education and training.

(c) RESOURCES.—In cases where the pilot program draws on existing infrastructure within the Department of Veterans Affairs, or relies on the supporting programs described in subsection (b), the Secretary shall take such actions as may be necessary to ensure those programs are expanded and resourced to accommodate increased usage from veterans participating in the pilot program. In addition to funding, such actions may include providing additional staff and resources to—

(1) provide administrative support to basic pilot program functions;

(2) ensure veteran success and ongoing engagement throughout online coursework; and

(3) support to connect graduates of the program to job opportunities within the federal government.

(d) DEFINITIONS.—In this section:

(1) WORK-BASED LEARNING.—The term “work-based learning" means sustained interactions with industry or community professionals in real workplace settings, to the extent practicable, or simulated environments at an educational institution that foster in-depth, firsthand engagement with the tasks required in a given career field, that are aligned to curriculum and instruction.

(2) PORTABLE CREDENTIAL.—The term “portable credential” means a documented award by a responsible and authorized body that has determined that an individual has achieved specific learning outcomes relative to a given standard. Credential in this context is an umbrella term that includes degrees, diplomas, licenses, certificates, badges, and professional/industry certifications. The credential—

(A) has value locally and nationally in labor markets, educational systems, and/or other contexts;

(B) is useable in a variety of environments, and the content and competencies the credential represents remain intact and are accessible by credential consumers; and

(C) enables earners to move vertically and horizontally within and across the credentialing ecosystem for attainment of other credentials.

## SEC. 8. PERSONNEL SECURITY CLEARANCES FOR CYBER ROLES.

(a) EXPEDITED PERSONNEL CLEARANCES FOR CYBER EXCEPTED SERVICE.—Section 3001 of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341) is amended by adding at the end the following new subsection:

"(k) EXPEDITING CLEARANCES UNDER CYBER EXCEPTED SERVICE.—

"(1) IN GENERAL.—The Secretary of Defense may prescribe a process for expediting the completion of the background investigations necessary for granting security clearances for any individual who is hired as an employee of the Department of Defense under the Cyber Excepted Service authorized in 10 U.S.C. 1599f for a position for which a security clearance is required.

"(2) REQUIRED FEATURES.—The process developed under subsection (a) shall provide for the following:

"(A) Quantification of the requirements for background investigations necessary for grants of security clearances for Department of Defense personnel and Department of Defense contractor personnel.

"(B) Categorization of personnel on the basis of the degree of sensitivity of their duties and the extent to which those duties are critical to the national security.

"(C) Prioritization of the processing of background investigations on the basis of the categories of personnel determined under subparagraph (B).

"(3) ANNUAL REVIEW.— The Secretary shall conduct an annual review of the process prescribed under paragraph (1) and shall revise that process as determined necessary in relation to ongoing Department of Defense missions.

"(4) CONSULTATION REQUIREMENT.— The Secretary shall consult with the Secretaries of the military departments and the heads of Defense Agencies in carrying out this section.

"(5) SUNSET.—The requirements of this subsection shall sunset on January 1, 2026.".

(b) REPORT ON IMPACT OF CLEARANCES ON HIRING AND CYBER WORKFORCE RECRUITMENT.—

(1) IN GENERAL.—The Comptroller General of the United States shall conduct a review of the impact of security clearance processing and other elements of the hiring process on recruitment for the Federal cyber workforce. The review shall include—

(A) an estimation of the frequency with which candidates are deterred from pursuing government careers because of delays in issuing security clearances;

(B) an assessment of the effectiveness of current clearance processes at finding a balance between the national security priorities of filling cyber jobs and limiting insider threats;

(C) a recommendation for a lead agency for developing and implementing a plan for addressing systemic problems identified in subparagraphs (A) and (B); and

(D) any other matter the Comptroller General determines appropriate.

(2) DEADLINES.—Not later than December 31, 2021, the Comptroller General shall brief the congressional defense committees, as well as the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives, on the preliminary findings of the study under this section. The Comptroller General shall submit a final report to the congressional defense committees as well as the Committee on Homeland Security and Governmental Affairs of the Senate and the House Committee on Oversight and Reform of the House of Representatives within 60 days following such briefing.

**SEC. 9. LEADERSHIP ENGAGEMENT AND ACCOUNTABILITY FOR THE DIVERSITY OF THE CYBER WORKFORCE**

(a) DEFINITIONS.—In this section:

(1) CYBERSECURITY AGENCY.—The term "cybersecurity agency" means specific organizations engaged primarily in cyber operations, policy, and/or regulatory activity within—

(A) the Department of Defense;

(B) the Department of Homeland Security;

(C) the Department of Justice and the Federal Bureau of Investigation;

(D) the Department of State;

(E) the Department of Commerce;

(F) Federal Trade Commission;

(G) Securities and Exchange Commission; and

(H) any other Federal department or agency, or component organization within a department or agency, that is primarily engaged in cyber operations, policy, and/or regulatory activity.

(2) DIVERSITY.—The term "diversity" means diversity of persons based on gender, race, ethnicity, disability status, veteran status, sexual orientation, gender identity, national origin, and other demographic categories.

(b) REWARD AND RECOGNIZE EFFORTS TO PROMOTE DIVERSITY AND INCLUSION.—

(1) IN GENERAL.—Each cybersecurity agency shall implement performance and advancement requirements that reward and recognize the efforts of individuals in senior positions and supervisors in the cybersecurity agency in fostering an inclusive environment and cultivating talent consistent with merit system principles, such as through participation in mentoring programs or sponsorship initiatives, recruitment events, and other similar opportunities.

(2) OUTREACH EVENTS.—Each cybersecurity agency shall create opportunities for individuals in senior positions and supervisors in the cybersecurity agency to participate in outreach events and to discuss issues relating to diversity and inclusion with the cyber workforce on a regular basis, including with employee resource groups.

(c) EXPAND TRAINING ON BIAS, INCLUSION, AND FLEXIBLE WORK POLICIES.—

(1) IN GENERAL.—Each cybersecurity agency shall—

(A) expand the provision of training on bias, including implicit or unconscious bias, micro-inequities, inclusion, and flexible work policies to the workforce of the cybersecurity agency; and

(B) make micro-inequities and bias training, including on implicit or unconscious bias, mandatory for—

(i) individuals in senior positions in the cybersecurity agency;

(ii) other individuals holding management positions in the cybersecurity agency; and

(iii) individuals in positions at the cybersecurity agency having responsibilities relating to outreach, recruitment, hiring, career development, promotion, or security clearance adjudication.

(2) PHASED IMPLEMENTATION.—The provision of training required under paragraph (1) may be implemented in a phased approach commensurate with the resources of the cybersecurity agency.

(3) LOW INCLUSION SCORES.—Each cybersecurity agency shall make available training on implicit or unconscious bias for members of the workforce of a bureau, directorate, division, office, or other component of the cybersecurity agency the inclusion scores of which, such as those measured by the New Inclusion Quotient index score, rank below the average for the cybersecurity agency for a period of three years or longer.

(4) BEST PRACTICES.—Each cybersecurity agency shall give special attention to ensuring the continuous incorporation of research-based best practices in training provided under this subsection, including best practices relating to addressing the intersection between certain demographics and job positions.

## 2.1 Create a Cyber Bureau and Assistant Secretary at the U.S. Department of State

This proposal implements the Commission's recommendation to create the Bureau of Cyberspace Security and Emerging Technologies within the U.S. Department of State. The head of the Bureau will be an Assistant Secretary and shall have experience in international diplomacy and cyber issues. The duties of this person will be to promote the United States' policy as it relates to cyberspace. The Bureau will not replace the overseas work of other agencies, but rather will ensure the coherence of U.S. efforts abroad and ensure the alignment of these efforts with U.S. national strategy. The number of authorized Assistant Secretaries is increased by one.

---

**A BILL**

To establish a Bureau of Cyberspace Security and Emerging Technologies within the United States Department of State and an Assistant Secretary of State to lead that Bureau, and for other purposes.

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

**SEC. 1. ORGANIZATION OF STATE.**

(a) Section 2305(b)(1) of Public Law 105-277 (22 U.S.C. 2651a(c)(1)), is amended—

(1) in subsection (c), paragraph (1) by striking "24," before "Assistant Secretaries," and by inserting "25";

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

(3) by inserting after subsection (f) the following new subsection (g):

"(g) BUREAU OF CYBERSPACE SECURITY AND EMERGING TECHNOLOGIES.—

"(1) IN GENERAL.— There is established, within the Department of State, a Bureau of Cyberspace Security and Emerging Technologies (referred to in this subsection as the 'Bureau'). The head of the Bureau shall be an Assistant Secretary and shall be appointed by the President, by and with the advice and consent of the Senate.

"(2) DUTIES.—

"(A) IN GENERAL.—The head of the Bureau shall perform such duties and exercise such powers as the Secretary of State shall prescribe, and as prescribed in paragraph (B) below.

"(B) DUTIES DESCRIBED.—The principal duties and responsibilities of the head of the Bureau shall be—

"(i) to serve as the principal cyberspace policy official within the Department of State and as the adviser to the Secretary of State for cyberspace issues;

"(ii) to lead the Department of State's diplomatic cyberspace efforts, which may include the promotion of human rights, democracy, and the rule of law, to include freedom of expression, innovation, communication, and economic prosperity, while respecting privacy and guarding against deception, fraud, and theft;

"(iii) to advocate for norms of responsible behavior in cyberspace and confidence building measures, deterrence, international responses to cyber threats, Internet freedom, digital economy, cybercrime, and capacity building;

"(iv) to promote an open, interoperable, reliable, and secure information and communications technology infrastructure globally;

"(v) to represent the Secretary of State in interagency efforts to develop and advance the policy priorities of the United States as it relates to cyberspace and emerging technologies; and

"(vi) to consult, as appropriate, with other Executive agencies with related functions vested in such Executive agencies by law.

"(3) QUALIFICATIONS.—The head of the Bureau shall be an individual of demonstrated competency in the fields of—

"(A) cybersecurity and other relevant cyber issues; and

"(B) international diplomacy.

"(4) ORGANIZATIONAL PLACEMENT.—During the four-year period beginning on the date of the enactment of this amendment, the head of the Bureau shall report to the Under Secretary for Political Affairs or, if directed by the Secretary, to an official holding a higher position than the Under Secretary for Political Affairs in the Department of State. After the conclusion of such period, the head of the Bureau shall report to an appropriate Under Secretary or to an official holding a higher position than Under Secretary.".

## 2.1.4 Increase Administrative Subpoena Authority for the U.S. Department of Justice

This proposal implements the Commission's recommendation to improve international tools for law enforcement activities in cyberspace, providing additional administrative subpoena authority to the U.S. Department of Justice.

---

**A BILL**

To provide administrative subpoena authority to improve law enforcement activities in cyberspace.

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

**SEC. 1. ADMINISTRATIVE SUBPOENAS.**

(a) Section 3486(a) of chapter 223 of title 18, United States Code, is amended—

(1) in paragraph (1)(A)(i)—

(A) in subclause (I), by striking "or";

(B) in subclause (II), by striking ", the Attorney General"; and

(C) by adding at the end the following new subclauses:

"(III) a criminal matter in which the assistance of the United States is required under a mutual legal assistance agreement or treaty; or (IV) a violation of section 1030, the Attorney General;";

(2) in paragraph (1)(C)—

(A) by inserting ", a mutual legal assistance agreement or treaty, or an investigation of a violation of section 1030" before "shall not extend beyond—"; and

(B) by inserting after subparagraph (1)(C) the following new subparagraph:

"(D) An administrative subpoena issued under subclauses III and IV of subsection (a)(1)(A)(i) shall be subject to the same prohibitions

and exceptions for disclosure as in subsection (c) and (d) of section 2709.";

(3) by redesignating subparagraph (D) of paragraph (1)(D) as subparagraph (E);

(4) in paragraph (1)(E), as so redesignated—

(A) in clause (i), by striking "and" after "18 years;"

(B) in clause (ii), by striking "." after "(42 U.S.C. 16901 et seq.)" and inserting "; and"; and

(C) by adding at the end the following new clause:

"(iii) the term "mutual legal assistance agreement or treaty" means either a treaty between the United States and a foreign country or countries, or an executive agreement made in accordance with section 2523."; and

(5) in paragraph (9), by inserting ", (1)(A)(i)(III)," after "paragraph (1)(A)(i)(II)".

## 2.1.5 Impose Sanctions for Foreign Election Interference

This proposal implements the Commission's recommendation to codify Executive Order 13848 on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election. As drafted, this proposal would create a new section within Title 50.

---

**A BILL**

To impose certain sanctions in the event of foreign interference in a United States Election, and for other purposes.

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

**SEC. 1709. Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election.**

(a) ASSESSMENT AND REPORT ON FOREIGN ELECTION INTERFERENCE.—

(1) ASSESSMENT.—

(A) IN GENERAL.—Not later than 45 days after the conclusion of a United States Election, the Director of National Intelligence shall conduct an assessment of any information indicating that a foreign government, or any person acting as an agent of or on behalf of a foreign government, has acted with the intent or purpose of interfering in an election.

(B) CONSULTATION.—In conducting the assessment required by this paragraph, the Director shall consult with any executive department and agency that the President, or in the absence of Presidential direction, the Director, determines should be consulted.

(C) CONTENTS.—The assessment required by this paragraph shall identify, to the maximum extent ascertainable, the nature of any foreign interference and any methods employed to execute it, the persons involved, and the foreign government or governments that authorized, directed, sponsored, or supported it.

(D) SUBMISSION.—The Director of National Intelligence shall deliver this assessment and appropriate supporting information to the President, the Secretary of State, the Secretary of the Treasury, the Secretary of

Defense, the Attorney General, and the Secretary of Homeland Security.

(2) REVIEW OF ASSESSMENT AND CREATION OF REPORT.—Within 45 days of receiving the assessment and information described in subsection (a)(1), the Attorney General and the Secretary of Homeland Security, in consultation with the heads of any other appropriate agencies and, as appropriate, State and local officials, shall deliver to the Congress, President, the Secretary of State, the Secretary of the Treasury, and the Secretary of Defense a report evaluating, with respect to the United States election that is the subject of the assessment—

(A) the extent to which any foreign interference that targeted election infrastructure materially affected the security or integrity of that infrastructure, the tabulation of votes, or the timely transmission of election results;

(B) if any foreign interference involved activities targeting the infrastructure of, or pertaining to, a political organization, campaign, or candidate, the extent to which such activities materially affected the security or integrity of that infrastructure, including by unauthorized access to, disclosure or threatened disclosure of, or alteration or falsification of, information or data;

(C) whether there are any material issues of fact with respect to the matters contained in the report that the Attorney General and the Secretary of Homeland Security are unable to evaluate or reach agreement on at the time the report is submitted; and

(D) any updates and recommendations, when appropriate, regarding remedial actions to be taken by the United States Government, other than the sanctions described in subsections (b) and (c).

(3) SUPPORT BY OTHER AGENCIES.—The heads of all relevant agencies shall transmit to the Director of National Intelligence any information relevant to the execution of the Director's duties pursuant to subsection (a)(1).

(4) AMENDMENT OF REPORT(S).—If relevant information emerges after the submission of the report mandated by subsection (a)(1), the Director, in consultation with the heads of any other appropriate agencies, shall amend the report, as appropriate, and the Attorney General and the Secretary of Homeland Security shall amend the report required by subsection (a)(2), as appropriate.

(5) NONAPPLICATION TO APPROPRIATE OFFICIALS.—Nothing in this section shall prevent the head of any agency or any other appropriate official from tendering to the President, at any time through an appropriate channel, any analysis, information, assessment, or evaluation of foreign interference in a United States election.

(6) INCLUSION OF INFORMATION ON ELECTION INTERFERENCE.—If information indicating that foreign interference in a State, tribal, or local election within the United States has occurred is identified, it may be included, as appropriate, in the assessment mandated by subsection (a)(1) or in the report mandated by subsection (a)(2) of this section, or submitted to the President in an independent report.

(7) FRAMEWORK.—Not later than 30 days following the enactment of this section, the Secretary of State, the Secretary of the Treasury, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence shall agree on a framework for the process that will be used to carry out their respective responsibilities pursuant to this section. The framework, which may be classified in whole or in part, shall focus on ensuring that agencies fulfill their responsibilities pursuant to section in a manner that maintains methodological consistency; protects law enforcement or other sensitive information and intelligence sources and methods; maintains an appropriate separation between intelligence functions and policy and legal judgments; ensures that efforts to protect electoral processes and institutions are insulated from political bias; and respects the principles of free speech and open debate.

(b) SANCTIONS FOR FOREIGN ELECTION INTERFERENCE.—

(1) SANCTIONED PROPERTY.—All property and interests in property that are in the United States, that hereafter come within the United States, or that are or hereafter come within the possession or control of any United States person of the following persons are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt in: any foreign person determined by the Secretary of the Treasury, in consultation with the Secretary of State, the Attorney General, and the Secretary of Homeland Security:

(A) to have directly or indirectly engaged in, sponsored, concealed, or otherwise been complicit in foreign interference in a United States election;

(B) to have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, any activity described in subsection (b)(1)(A) or any person whose

property and interests in property are blocked pursuant to this subsection; or

(C) to be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property or interests in property are blocked pursuant to this subsection.

(2) NONAPPLICATION TO EXECUTIVE OFFICIALS.—Nothing in this section shall be construed as a limitation on the Secretary of the Treasury or other executive officials from exercising their authority under the International Emergency Economic Powers Act, 50 U.S.C. 1701 *et seq.*, the National Emergencies Act 50 U.S.C. 1601 *et seq.*, the Immigration and Nationality Act of 1952 8 U.S.C. 1182(f); and 3 U.S.C. 301, or any other authorization.

(3) NONAPPLICATION TO CONTRACTS OR LICENSES.—The prohibitions in subsection (b)(1) apply notwithstanding any contract entered into or any license or permit granted prior to the implementation date of this section.

(c) IMPLEMENTATION OF SANCTIONS.—Following the transmission of the assessment mandated by subsection (a)(1) and the report mandated by subsection (a)(2):

(1) The Secretary of the Treasury shall review the assessment mandated by subsection (a)(1) and the report mandated by subsection (a)(2), and, in consultation with the Secretary of State, the Attorney General, and the Secretary of Homeland Security, impose all appropriate sanctions pursuant to subsection (b) of this section.

(2) The Secretary of State and the Secretary of the Treasury, in consultation with the heads of other appropriate agencies, shall jointly prepare a recommendation for the President as to whether additional sanctions against foreign persons may be appropriate in response to the identified foreign interference and in light of the evaluation in the report mandated by subsection (a)(2), including—

(A) an assessment of the effect of the recommended sanctions on the economic and national security interests of the United States and its allies;

(B) a conclusion as to whether recommended sanctions are appropriately calibrated to the scope of the foreign interference identified; and

(C) as appropriate, proposed sanctions with respect to the largest business entities licensed or domiciled in a country whose government authorized, directed, sponsored, or supported election interference,

including at least one entity from each of the following sectors: financial services, defense, energy, technology, and transportation (or, if inapplicable to that country's largest business entities, sectors of comparable strategic significance to that foreign government) and may include one or more of the following with respect to each targeted foreign person—

(i) blocking and prohibiting all transactions in a person's property and interests in property subject to United States jurisdiction;

(ii) export license restrictions under any statute or regulation that requires the prior review and approval of the United States Government as a condition for the export or re-export of goods or services;

(iii) prohibitions on United States financial institutions making loans or providing credit to a person;

(iv) restrictions on transactions in foreign exchange in which a person has any interest;

(v) prohibitions on transfers of credit or payments between financial institutions, or by, through, or to any financial institution, for the benefit of a person;

(vi) prohibitions on United States persons investing in or purchasing equity or debt of a person;

(vii) exclusion of a person's alien corporate officers from the United States;

(viii) imposition on a person's alien principal executive officers of any of the sanctions described in this section; or

(ix) any other measures authorized by law.

(d) EXPLANATION OF PROHIBITIONS.—The prohibitions in subsection (b) include the following:

(1) The making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any person whose property and interests in property are blocked pursuant to this section.

(2) The receipt of any contribution or provision of funds, goods, or services from any such person.

(e) AVOIDANCE OF SANCTIONS.—

(1) EVASIONS AND VIOLATIONS.—Any transaction that evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions set forth in this section is prohibited.

(2) CONSPIRACY.—Any conspiracy formed to violate any of the prohibitions set forth in this section is prohibited.

(f) DEFINITIONS.—For the purposes of this section:

(1) PERSON.—The term "person" means an individual or entity.

(2) ENTITY.—The term "entity" means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization.

(3) UNITED STATES PERSON.—The term "United States person" means any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person (including a foreign person) in the United States.

(4) ELECTION INFRASTRUCTURE.—The term "election infrastructure" means information and communications technology and systems used by or on behalf of the Federal government or a State or local government in managing the election process, including voter registration databases, voting machines, voting tabulation equipment, and equipment for the secure transmission of election results.

(5) UNITED STATES ELECTION.—The term "United States election" means any election for Federal office held on, or after, the enactment date of this section.

(6) FOREIGN INTERFERENCE.—The term "foreign interference," with respect to an election, includes any covert, fraudulent, deceptive, or unlawful actions or attempted actions of a foreign government, or of any person acting as an agent of or on behalf of a foreign government, undertaken with the purpose or effect of influencing, undermining confidence in, or altering the result or reported result of, the election, or undermining public confidence in election processes or institutions.

(7) FOREIGN GOVERNMENT.—The term "foreign government" means any national, state, provincial, or other governing authority, any political party, or any official of any governing authority or political party, in each case of a country other than the United States.

(8) COVERT.—The term "covert," with respect to an action or attempted action, means characterized by an intent or apparent intent that the role of a foreign government will not be apparent or acknowledged publicly.

(9) STATE.—The term "State" means the several States or any of the territories, dependencies, or possessions of the United States.

(g) NOTICE. —No prior notice of a listing or determination made pursuant to subsection (b) is required.

(h) NO LIMITATION ON UNITED STATES.—Nothing in this section prohibits transactions for the conduct of the official business of the United States Government by employees, grantees, or contractors thereof.

(i) RULEMAKING.—The Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, is authorized to take such actions, including the promulgation of rules and regulations as may be necessary to carry out the purposes of this section.

(j) REPORT TO CONGRESS.—The Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, shall submit an initial report, and within each calendar afterwards an annual report, to the Congress on any instance where a sanction is being imposed under this section.

(k) RULE OF CONSTRUCTION.—This section shall be construed and implemented consistent with the limitations contained in paragraphs (1) and (3) of section 203(b)of the International Emergency Economic Powers Act (Public Law 95–223; 50 U.S.C. 1702(b)), as amended.

(l) CONSTRUCTION.—

(1) NON IMPAIRMENT.—Except as explicitly stated in this section, nothing in this section shall be construed to impair or otherwise affect—

(A) the authority granted by law to an executive department or agency, or the head thereof; or

(B) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(2) NO CREATION OF BENEFITS.—This section is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(3) EXCLUSION OF UNITED STATES PERSONS.—Nothing in this section shall be construed to require sanctions or punitive measures against United States persons.

(m) CASE-BY-CASE WAIVER OF AUTHORITY.—

(1) IN GENERAL.—The President may waive, on a case-by-case basis and for a period of not more than 180 days, a requirement under this section to impose or maintain sanctions with respect to a person, and may waive the continued imposition of such sanctions, not less than 30 days after the President determines and reports to the appropriate congressional committees that it is vital to the national security interests of the United States to waive such sanctions.

(2) RENEWAL OF WAIVERS.—The President may, on a case-by-case basis, renew a waiver under paragraph (1) for an additional period of not more than 180 days if, not later than 15 days before that waiver expires, the President makes the determination and submits to the appropriate congressional committees a report described in paragraph (1).

(3) SUCCESSIVE RENEWAL.—The renewal authority provided under paragraph (2) may be exercised for additional successive periods of not more than 180 days if the President follows the procedures set forth in paragraph (2), and submits the report described in paragraph (1), for each such renewal.

(n) CONTENTS OF WAIVER REPORTS.—Each report submitted under subsection (m) in connection with a waiver of sanctions under this section with respect to a person, or the renewal of such a waiver, shall include—

(1) a specific and detailed rationale for the determination that the waiver is vital to the national security interests of the United States;

(2) a description of the activity that resulted in the person being subject to sanctions;

(3) an explanation of any efforts made by the United States, as applicable, to secure the cooperation of the government with primary jurisdiction over the person or the location where the activity described in paragraph (2) occurred in terminating or, as appropriate, penalizing the activity; and

(4) an assessment of the significance of the activity described in paragraph (2) in contributing to the ability of Iran to threaten the interests of the United States or allies of the United States, develop systems capable of delivering

weapons of mass destruction, support acts of international terrorism, or violate the human rights of any person in Iran.

(o) EFFECT OF REPORT ON WAIVER.—If the President submits a report under subsection (m) in connection with a waiver of sanctions under this section with respect to a person, or the renewal of such a waiver, the President shall not be required to impose or maintain sanctions under this section, with respect to the person described in the report during the 30-day period referred to in subsection (a).

# 3.1 & 3.1.1 Codify Sector-Specific Agencies as Sector Risk Management Agencies and Establish a National Risk Management Cycle

This proposal codifies Sector-specific Agencies as Sector Risk Management Agencies and assigns more concrete responsibilities and baseline expectations (3.1). The proposal also requires a four-year cycle of risk identification and assessment led by DHS, in coordination with SRMAs, that prompts and supports a National Critical Infrastructure Resilience Strategy led by the President (3.1.1).

---

**A BILL**

To codify Sector Risk Management Agencies and empower them to assess and mitigate sector-specific risk throughout the United States, to establish a four-year cycle of risk identification and assessment led by the United States Department of Homeland Security, and for other purposes.

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

**SEC. 1. SHORT TITLE.**

This Act may be cited as the "National Risk Management Act".

**SEC. 2. DEFINITIONS.**

In this Act:

(1) CRITICAL INFRASTRUCTURE.—The term "critical infrastructure" has the meaning given that term in section 1016 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (42 U.S.C. 5195c).

(2) NATIONAL CRITICAL FUNCTIONS.—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.

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

(4) DIRECTOR.—The term "Director" means the Director of the Cybersecurity and Infrastructure Security Agency of the Department.

(5) SECRETARY.—The term "Secretary" means the Secretary of Homeland Security.

(6) SECTOR RISK MANAGEMENT AGENCY.—The term "Sector Risk Management Agency" means an agency so-designated under section 5.

## SEC. 3. NATIONAL RISK MANAGEMENT CYCLE.

(a) RISK IDENTIFICATION AND ASSESSMENT.—

(1) 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.

(2) CONSULTATION.—In developing the process required by paragraph (1), the Secretary shall consult with Sector Risk Management Agencies and critical infrastructure owners and operators.

(3) PUBLICATION.—Not later than 180 days following the enactment of this Act, the Secretary shall publish procedures for process developed pursuant to paragraph (1) in the Federal Register.

(4) REPORT.—Not later than one year following the enactment of this Act, and every four years thereafter, the Secretary shall submit to the President a report on the risks identified by the process established pursuant to paragraph (1).

(b) NATIONAL CRITICAL INFRASTRUCTURE RESILIENCE STRATEGY.—

(1) IN GENERAL.—Not later than one year after the Secretary delivers each report required by subsection (a), the President shall deliver to Majority and Minority Leaders of the Senate and the Speaker and Minority Leader of the House of Representatives a National Critical Infrastructure Resilience Strategy designed to address the risks identified by the Secretary.

(2) ELEMENTS.—In each strategy delivered pursuant to this subsection, the President shall:

(A) Identify, assess, and prioritize areas of risk to critical infrastructure that would compromise, disrupt, or impede their ability to support the national critical functions of national security, economic security, or public health and safety.

(B) Assess the implementation of the previous National Critical Infrastructure Resilience Strategy, as applicable.

(C) Identify and outline current and proposed national-level actions, programs, and efforts to be taken to address the risks identified.

(D) Identify the Federal departments or agencies responsible for leading each national-level action, program, or effort and the relevant critical infrastructure sectors for each.

(E) Outline the budget plan required to provide sufficient resources to successfully execute the full range of activities proposed or described by the National Critical Infrastructure Resilience Strategy.

(F) Request any additional authorities or resources necessary to successfully execute the National Critical Infrastructure Resilience Strategy.

(3) FORM.—The strategy required in subsection (a) shall be unclassified, but may contain a classified annex.

(c) CONGRESSIONAL BRIEFING.—Not later than one year after the President delivers each National Critical Infrastructure Resilience Strategy, and every year thereafter, the Secretary, in coordination with Sector Risk Management Agencies, shall brief the appropriate committees of Congress on the national risk management cycle activities undertaken pursuant to this section.

## SEC. 4. CRITICAL INFRASTRUCTURE SECTOR DESIGNATION.

(a) INITIAL REVIEW.—Within 180 days following the enactment of this section, the Secretary shall review the current critical infrastructure sector model and corresponding designations for Sector Risk Management Agencies and submit a report to the President containing recommendations for—

(1) any additions or deletions to the list of critical infrastructure sectors set forth in Presidential Policy Directive 21; and

(2) any new assignment or alternative assignment of a Federal department or agency to serve as the Sector Risk Management Agency for a sector.

(b) PERIODIC REVIEW.—One year before the delivery of each strategy required pursuant to section 2, the Secretary, in consultation with the Director, shall—

(1) review the current list of critical infrastructure sectors and the assignment of Sector Risk Management Agencies, as set forth in Presidential Policy Directive 21, or any successor document; and

(2) recommend to the President—

(A) any additions or deletions to the list of critical infrastructure sectors; and

(B) any new assignment or alternative assignment of a Federal agency to serve as the Sector Risk Management Agency for each sector.

(c) UPDATE.—

(1) IN GENERAL.—Not later than 180 days following a recommendation by the Secretary pursuant to subsection (b), the President shall—

(A) review the recommendation and update, as appropriate, the designation of critical infrastructure sectors and each sector's corresponding Sector Risk Management Agency; or

(B) submit a report to the Majority and Minority Leaders of the Senate and the Speaker and Minority Leader of the House of Representatives explaining the basis for rejecting the recommendations of the Secretary.

(2) LIMITATION.—The President—

(A) may not designate more than one department or agency as the Sector Risk Management Agency for each critical infrastructure sector; and

(B) may only designate an agency under this subsection if the agency is referenced in section 205 of the Chief Financial Officers Act of 1990 (42 U.S.C. 901).

(d) PUBLICATION.—Any designation of critical infrastructure sectors shall be published in the Federal Register.

**SEC. 5. SECTOR RISK MANAGEMENT AGENCIES.**

(a) IN GENERAL.—Any reference to a Sector-Specific Agency in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Sector Risk Management Agency of the relevant critical infrastructure sector.

(b) COORDINATION.—In carrying out this section, Sector Risk Management Agencies shall—

(1) coordinate with the Department and other relevant Federal departments and agencies;

(2) collaborate with critical infrastructure owners and operators; and

(3) as appropriate, coordinate with independent regulatory agencies, and State, local, tribal, and territorial entities.

(c) RESPONSIBILITIES.— Each Sector Risk Management Agency shall utilize its specialized expertise about its assigned critical infrastructure sector and authorities under applicable law to support and carry out activities for its assigned sector related to:

(1) Sector risk management, including—

(A) establishing and carrying out programs to assist critical infrastructure owners and operators within their assigned sector in identifying, understanding, and mitigating threats, vulnerabilities, and risks to their region, sector, systems or assets; and

(B) recommending resilience measures to mitigate the consequences of destruction, compromise, and disruption of their systems and assets.

(2) Sector risk identification and assessment, including—

(A) identifying, assessing, and prioritizing risks to critical infrastructure within their sector, considering physical and cyber threats, vulnerabilities, and consequences; and

(B) supporting national risk assessment efforts led by the Department, including identifying, assessing, and prioritizing cross-sector and national-level risks.

(3) Sector coordination, including—

(A) serving as a day-to-day Federal interface for the dynamic prioritization and coordination of sector-specific activities and their responsibilities under this section;

(B) serving as the government coordinating council chair for their assigned sector; and

(C) participating in cross-sector coordinating councils, as appropriate.

(4) Threat and vulnerability information sharing, including—

(A) facilitating access to, and exchange of, information and intelligence necessary to strengthen the resilience of critical infrastructure,

including through the sector's information sharing and analysis center;

(B) facilitating the identification of intelligence needs and priorities of critical infrastructure in coordination with the Office of Director of National Intelligence and other Federal departments and agencies, as appropriate;

(C) providing the Director ongoing, and where practicable, real-time awareness of identified threats, vulnerabilities, mitigations, and other actions related to the security of critical infrastructure; and

(D) supporting the reporting requirements of the Department of Homeland Security under applicable law by providing, on an annual basis, sector-specific critical infrastructure information.

(5) Incident management, including—

(A) supporting incident management and restoration efforts during or following a security incident;

(B) supporting the Cybersecurity and Infrastructure Security Agency, as requested, in conducting vulnerability assessments and asset response activities for critical infrastructure; and

(C) supporting the Attorney General and law enforcement agencies with efforts to detect and prosecute threats to and attacks against critical infrastructure.

(6) Emergency preparedness, including—

(A) coordinating with critical infrastructure owners and operators in the development of planning documents for coordinated action in response to an incident or emergency;

(B) conducting exercises and simulations of potential incidents or emergencies; and

(C) supporting the Department and other Federal departments or agencies in developing planning documents or conducting exercises or simulations relevant to their assigned sector.

(7) Participation in national risk management efforts, including—

(A) supporting the Secretary in the risk identification and assessment activities carried out pursuant to section 2 of this Act;

(B) supporting the President in the development of the National Critical Infrastructure Resilience Strategy pursuant to section 2 of this Act; and

(C) implementing the National Critical Infrastructure Resilience Strategy pursuant to section 2 of this Act.

(d) STATUS OF INFORMATION.–Information shared with a Sector Risk Management Agency in furtherance of the responsibilities outlined in subsection (c)(2)(B) shall be treated as protected critical infrastructure information under section 214 of the Homeland Security Act of 2002 (6 U.S.C. 673).

**SEC. 6 REPORTING AND AUDITING.**

(a) Not later than two years following the enactment of this Act, and every four years thereafter, the Government Accountability Office shall submit a report to appropriate Committees of Congress on the effectiveness of Sector Risk Management Agencies in carrying out their responsibilities under section 4 of this Act.

## 3.1.2 Establish a National Cybersecurity Assistance Fund

This proposal establishes a National Cybersecurity Assistance Fund for projects and programs aimed at systematically increasing the resilience of public and private entities, thereby increasing the overall resilience of the United States.

---

**A BILL**

To establish a National Cybersecurity Assistance Fund for projects and programs aimed at systematically increasing the resilience of public and private entities in the United States, and for other purposes.

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

**SEC. 1. SHORT TITLE.**

This Act may be cited as the "National Cybersecurity Assistance Fund Act".

**SEC. 2. DEFINITIONS**.

In this section:

(1) CRITICAL INFRASTRUCTURE.—The term "critical infrastructure" has the meaning given that term in section 1016(e) of Public Law 107-56 (42 U.S.C. 5195c(e)).

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

(3) SECRETARY.—The term "Secretary" means the Secretary of Homeland Security.

**SEC. 3. ESTABLISHMENT OF THE NATIONAL CYBERSECURITY ASSISTANCE FUND.**

There is established in the Treasury a National Cybersecurity Assistance Fund which shall be available to fund 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.

**SEC. 4. ADMINISTRATION OF GRANTS FROM THE NATIONAL CYBERSECURITY ASSISTANCE FUND.**

(a) IN GENERAL.—Pursuant to the requirements of this section, the Secretary, acting through the Administrator of the Federal Emergency Management Agency and the Director of the Cybersecurity and Infrastructure Security Agency, shall develop and administer processes to—

(1) establish focused grant programs to address identified areas of significant cybersecurity risk to critical infrastructure;

(2) accept and evaluate applications for each grant program;

(3) award grants under each grant program;

(4) and disburse funds from the National Cybersecurity Assistance Fund established pursuant to subsection (a).

(b) ELIGIBLE ENTITIES.—

(1) IN GENERAL.—The following entities shall be eligible to receive grants from the fund:

(A) a State, local, tribal or territorial government.

(B) a public owner or operator of critical infrastructure.

(C) a private owner or operator of critical infrastructure.

(2) LIMITATION.— No grant recipient shall be eligible to receive more than 1 grant from the fund in any fiscal year.

(c) ESTABLISHMENT OF RISK-FOCUSED GRANT PROGRAMS.—

(1) IN GENERAL.—The Secretary, acting through the Director of the Cybersecurity and Infrastructure Security Agency, shall establish at least one grant program focused on mitigating an identified category of significant national risk to critical infrastructure within the United States. Prior to choosing a focus area for a grant program pursuant to this paragraph, the Director shall ensure—

(A) there is a clearly-defined, critical, cybersecurity-related risk to be mitigated;

(B) market forces do not provide sufficient private-sector incentives to mitigate the risk without government investment, and

(C) there is clear Federal need, role, and responsibility to mitigate the risk.

(2) FUNDING.—

(A) RECOMMENDATION.—Beginning in the first fiscal year following the establishment of the National Cybersecurity Assistance Fund and each fiscal year thereafter, the Director of the Cybersecurity and Infrastructure Security Agency shall—

(i) assess the funds available in the National Cybersecurity Assistance Fund for the fiscal year; and

(ii) recommend to the Secretary the total amount of funding to be made available under each grant program established pursuant to this subsection.

(B) ALLOCATION.—After considering the recommendations made by the Director of the Cybersecurity and Infrastructure Security Agency pursuant to subparagraph (A), the Secretary shall allocate funds from the National Cybersecurity Assistance Fund to each active grant program established pursuant to this subsection.

(d) GRANT PROCESSES.—The Secretary, acting through the Administrator of the Federal Emergency Management Agency, shall—

(1) establish a process to receive grant applications from and award funds to eligible entities under the grant programs established pursuant to subsection (c); and

(2) require the submission of such information as the Secretary determines is necessary to—

(A) evaluate a grant application against the criteria established pursuant to this Act;

(B) disburse grant funds;

(C) provide oversight of disbursed grant funds; and

(D) evaluate the effectiveness of the funded project in increasing the overall cyber resilience of the United States.

(e) GRANT CRITERIA.— For each grant program established pursuant to subsection (c), the Secretary, acting through the Director of the Cybersecurity and Infrastructure Security Agency, shall develop and publish criteria for evaluating applications for funding. Such criteria shall consider—

(1) whether the application identifies a clearly-defined cybersecurity risk;

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

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

(4) the potential consequences of leaving the identified risk unmitigated, including the potential impact to national critical functions; and

(5) other appropriate factors identified by the Director.

(f) EVALUATION OF GRANTS APPLICATIONS.—

(1) IN GENERAL.—Utilizing the criteria established pursuant to subsection (e), the Director of the Cybersecurity and Infrastructure Security Agency shall evaluate grant applications made under each grant program established pursuant to subsection (c).

(2) RECOMMENDATION.—Following the evaluations required pursuant to paragraph (1), the Director of the Cybersecurity and Infrastructure Security Agency shall prepare a recommendation to the Secretary identifying applications for approval, including the amount of funding recommended for each such approval.

(g) AWARD OF GRANT FUNDING.—The Secretary shall—

(1) review the recommendations of the Director of the Cybersecurity and Infrastructure Security Agency prepared pursuant to subsection (f);

(2) shall accept or modify the recommended approvals and funding amounts; and

(3) provide a final determination of grant awards to the Administrator of the Federal Emergency Management Agency to be dispersed and administered under the process established pursuant to subsection (d).

**SEC. 5. EXIGENT AUTHORITY.**

If the Secretary identifies an urgent circumstance in which a timely investment would neutralize or substantially mitigate a significant cybersecurity threat to national security, economic security, or public health and safety, the Secretary may accept an application from eligible entities for a mitigation project and reallocate any available funds in the National Cybersecurity Assistance Fund toward responding to the threat, without regard for the focus areas of any active grant program established pursuant to this Act.

**SEC. 6. EVALUATION OF GRANT PROGRAMS UTILIZING THE NATIONAL CYBERSECURITY ASSISTANCE FUND.**

(a) EVALUATION—The Secretary shall establish a process to evaluate the effectiveness and efficiency of grants distributed to recipients and develop appropriate updates, as needed, to the grant programs.

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

(c) GRANT PROGRAM REVIEW.—

(1) ANNUAL ASSESSMENT.—Prior to start of the second fiscal year in which grants are awarded pursuant to this Act, and annually thereafter, the Director of the Cybersecurity and Infrastructure Security Agency shall assess the grant programs established pursuant to this Act and determine for the coming fiscal year—

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

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

(C) whether the scope of any existing grant program should be modified.

(2) SUBMISSION TO CONGRESS.—Not later than 90 days prior to the start of each fiscal year, the Secretary 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 the assessment

conducted pursuant to paragraph (1) and any planned alterations to the grant program for the coming fiscal year.

**SEC. 7. LIMITATION ON USE OF GRANT FUNDS.**

Funds awarded pursuant to this Act—

(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;

(B) by or for a non-U.S. entity; or

(C) for any recreational or social purpose.

**SEC. 8. AUTHORIZATION OF APPROPRIATIONS.**

There are authorized to be appropriated $XXXX to carry out this section in fiscal year 2021 and such sums as may be necessary through fiscal year 2031.

**SEC. 9. SUNSET**.

The authorities provided in this Act, including the reporting requirements, shall expire on September 30, 2032.

## 3.2 Implement and Maintain a Continuity of the Economy Plan

This proposed legislation would implement the Commission's recommendation to direct the President to coordinate with relevant Federal agencies to develop and maintain a Continuity of the Economy plan, in consultation with the private sector, to ensure the continuous operation of critical functions of the economy in the event of a significant cyber disruption. This plan will analyze national critical functions, prioritize response and recovery efforts, identify areas for investments in resilience, identify areas for preserving data, and expanding education and readiness of the general public.

---

**A BILL**

To establish a comprehensive plan to ensure the continuous operation of critical functions of the economy in the event of a significant cyber disruption, and for other purposes.

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

**SEC. 1. CONTINUITY OF THE ECONOMY PLAN.**

(a) IN GENERAL.— The President of the United States is directed to develop and maintain a Continuity of the Economy plan, in this section the "plan," to provide for the restoration of the United States economy in the event of a significant degradation of economic activity in the United States caused by a cyberattack or other significant event. The plan shall be consistent with an economy based on free markets, the rule of law, and shall respect private property rights.

(b) COORDINATION AND CONSULTATION.—In developing the plan required by subsection (a), the President shall—

(1) receive the advice from experts from the Department of Homeland Security and Department of Defense and any other executive branch agency that the President determines is necessary to complete the plan;

(2) receive the advice and expertise from Federal regulators, as appropriate; and

(3) consult with relevant critical infrastructure sectors through existing sector-coordinating councils, as appropriate.

(c) DEVELOPMENT OF PLAN. The plan required by subsection (a) shall—

(1) examine the national-level distribution of goods and services necessary for the reliable economic functioning of the United States;

(2) determine the most critical essential economic functions of the United States economy, to include, as appropriate, the distribution mechanisms, in each economic sector, including but not limited to—

(A) bulk power and electric transmission systems;

(B) national and international financial systems, to include wholesale payments, stocks, and currency exchanges;

(C) national and international communications networks, data-hosting, and cloud services;

(D) interstate oil and natural gas pipelines; and

(E) national-level and international trade, logistics, material, food, and medical distribution, to include road, rail, air, and maritime shipping;

(3) identify economic functions the disruption of which will cause catastrophic economic loss, loss of public confidence, the widespread imperilment of human life, or functions the disruption of which will undermine response, recovery, or mobilization efforts in a crisis;

(4) incorporate into the plan, to the extent practicable, the principles and practices contained within plans for the continuity of government and continuity of operations;

(5) review and determine where it would be most feasible and optimal to install parallel or stand-alone analogue services on select industrial control networks in the event that the interests of national security outweigh the benefits of dependence on internet connectivity;

(6) identify critical segments of the economy where the preservation of data in a protected, verified, and uncorrupted format would be required to quickly recover the economy in the face of significant disruption following a cyberattack;

(7) include a list of raw materials, industrial goods, and key services the absence of which would significantly undermine the ability of the United States to avoid or recover from an economic collapse and a recommendation as to whether the United States should maintain a strategic reserve of said material, goods, and service capability;

(8) consider the advisability and feasibility of mechanisms for extending the credit of the United States to key participants in the national economy when such credit would be necessary to avoid catastrophic economic collapse or

would allow the recovery from such a collapse;

(9) identify critical segments of the economy necessary to provide materiel and operational support to defense;

(10) consider any other matter which would aid in protecting and increasing the resilience of the national economy from a significant disruption;

(11) determine whether there exists sufficient authority for the Department of Homeland Security, the State National Guards, and the Department of Defense to use assets and capabilities to assist the nation in the recovery from an economic collapse; and

(12) review and assess the authorities of any other Federal agency the President determines necessary to evaluate whether there are sufficient authorities and capabilities to assist the nation in the event of a catastrophic economic collapse.

(d) SUBMISSION TO CONGRESS.—Not later than two years following the enactment of this Act, the President shall submit the plan required under subsection (a) to the Majority and Minority Leader of the Senate and the Speaker and the Minority Leader of the House of Representatives. In addition to the elements of the plan required pursuant to subsection (c), the submission to Congress shall include—

(1) any statutory changes necessary to carry out the plan; and

(2) any proposed budgetary changes or additional resources needed to—

(A) implement the plan; or

(B) maintain program offices and personnel necessary to maintain plans and conduct exercises, assessments and updates over time.

## 3.3 Codify a Cyber State of Distress and Establish a Cyber Response and Recovery Fund

This proposal implements the Commission's recommendation to codify a "Cyber State of Distress" in the event of, or in preparation for, a significant cyber incident or series of incidents to enable the Secretary of Homeland Security to coordinate asset preparation, response, and recovery operations. When this declaration is issued, responding Federal agencies will be able to increase, scale up, or augment the capabilities through a cyber response and recovery fund. This declaration is necessary to enable the Federal government to respond to significant cyber incidents that fall below an Emergency Declaration or Major Disaster.

---

**A BILL**

To establish a Cyber State of Distress declaration and a Cyber Response and Recovery Fund to enable the Secretary of Homeland Security to better assist critical infrastructure in preparing for, responding to, and recovering from a significant cyber incident, and for other purposes.

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

**SEC. 1. CYBER STATE OF DISTRESS DECLARATION.**

The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended by adding at the end the following:

"Subtitle C—Cyber State of Distress

**"SEC. 2226. CYBER STATE OF DISTRESS.**

"(a) DEFINITIONS.—In this section:

"(1) ASSET RESPONSE.—The term "asset response" means activities including—

"(A) furnishing technical and advisory assistance to entities affected by a cyber incident to protect their assets, mitigate vulnerabilities, and reduce the related impacts;

"(B) identifying other entities that may be at risk and assessing their risk to the same or similar vulnerabilities;

"(C) assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks;

"(D) facilitating information sharing and operational coordination with threat response; and

"(E) providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery.

"(2) DECLARATION.—The term "declaration" means a declaration issued pursuant to section (b).

"(3) INCIDENT.—The term "incident" has the meaning given that term in section 2209, defined as 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.

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

"(5) SIGNIFICANT CYBER INCIDENT.—The term "significant cyber incident" means an incident that is, or group of related cyber incidents that together are, reasonably likely to result in significant harm to the national security, foreign policy, or economic health or financial stability of the United States.

"(b) DECLARATION.—

"(1) IN GENERAL.—The Secretary is authorized to declare a cyber state of distress in accordance with this section if the Secretary determines that—

"(A) a significant cyber incident has occurred; or

"(B) there is a near-term risk of a significant cyber incident.

"(2) COORDINATION OF ACTIVITIES.—Upon declaration of a Cyber State of Distress, the Secretary shall—

"(A) coordinate all asset response activities by Federal agencies in response to a cyber state of distress;

"(B) shall harmonize such activities with asset response activities of private entities and State and local governments to the maximum extent practicable; and

"(C) shall harmonize such activities with Federal, State, local, tribal, and territorial law enforcement investigations and threat response activities.

"(3) DURATION.—A declaration made pursuant to this subsection shall be for a period the Secretary designates or 60 days, whichever is shorter.

"(4) RENEWAL.—The Secretary may renew a declaration made pursuant to this subsection, as necessary to respond to or prepare for a significant cyber incident.

"(5) PUBLICATION.—A declaration under this subsection shall be published in the Federal Register within 72 hours of being issued.

"(6) LIMITATION ON DELEGATION.—The Secretary may not delegate the authority to declare a cyber state of distress.

"(7) SUPERSEDING DECLARATIONS.—A declaration made pursuant to this subsection shall have no effect if the President makes a disaster declaration pursuant to the Stafford Act (42 U.S.C. 5122 et seq.).

"(c) ADVANCE ACTIVITIES.—The Secretary shall assess the Federal resources available to respond to a declared cyber state of distress and shall take actions to arrange or procure such additional resources as the Secretary determines necessary, including, if necessary, entering into standby contracts for private-sector cybersecurity services or incident responders.

"(d) CYBER RESPONSE AND RECOVERY FUND.—

"(1) ESTABLISHMENT.—There is hereby established in the Treasury a Cyber Response and Recovery Fund, which shall be available to carry out—

"(A) activities related to a cyber state of distress declared by the Secretary pursuant to subsection (a); and

"(B) advance activities undertaken by the Secretary of Homeland Security pursuant to section (c).

"(2) EXPENDITURES OUT OF THE CYBER RESPONSE AND RECOVERY FUND.—The cost of any assistance provided pursuant to this section shall be

reimbursed out of funds appropriated to the Cyber Response and Recovery Fund and made available to carry out this section.".

**SEC. 2. CLERICAL AMENDMENT.**

The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by adding at the end the following new items:

"Subtitle C—Cyber State of Distress

"Sec. 2226. Cyber State of Distress."

## 3.3.2 Clarify Liability for Federally Directed Mitigation, Response, and Recovery Efforts

Congress should pass a law specifying that entities taking, or refraining from taking, action at the duly authorized direction of any agency head, or any other Federal official authorized by law, should be insulated from legal liability. Covered actions should include any request or order by relevant Federal agencies issued to protect against or respond to an emergency or threat relating to a cybersecurity incident impacting national security.

---

**A BILL**

To clarify liability for Federally directed mitigation, response, and recovery efforts following a cybersecurity incident impacting national security, and for other purposes.

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

**SEC. 1. LIABILITY PROTECTION FOR COMPLIANCE WITH A FEDERAL NATIONAL SECURITY REQUEST OR ORDER.**

(a) DEFINITIONS.—In this section:

(1) COVERED ACTIVITY.—The term "covered activity" means any instance in which a covered owner or operator takes, or refrains from taking, an action related to cybersecurity or physical security pursuant to a request or order, made in writing, by the—

(A) Secretary of Homeland Security;

(B) Secretary of Defense;

(C) Secretary of Energy;

(D) the Attorney General; or

(E) their respective designees.

(2) COVERED ENTITY.—The term "covered entity" means any entity, including its parent, subsidiaries, owners, operators, or members, or Federal or State, local, tribal, or territorial entity, that is a critical infrastructure, as that term is defined in section 1016(e) of Public Law 107-56 (42 U.S.C. 5195c(e)), including, but not limited to the following sectors:

(A) Communications.

(B) Energy.

(C) Transportation Systems.

(D) Water and Wastewater Systems.

(b) LIABILITY PROTECTION FOR COVERED ENTITIES.—Notwithstanding any other provision of law, no covered entity, as defined in subsection (a)(2) above, shall be liable for civil damages or other fines or penalties, and no cause of action shall lie or be maintained in any court or administrative agency, as a result of a covered activity, as defined in subsection (a)(1) above, provided—

(1) the entity was acting pursuant to and within the scope of the request or order for a subsection (a)(1) covered activity; and

(2) the damages, fines or penalties are not the result of willful misconduct, criminal conduct, gross negligence, or reckless misconduct.

(c) BURDEN OF PROOF.—In an action for misconduct or negligence listed under subsection (b)(2) against a covered entity for covered activity taken pursuant to this section, the plaintiff or regulatory agency shall have the burden of proving by clear and convincing evidence for such misconduct or negligence by each covered entity and that such misconduct or negligence caused the harm for which damages, fines or penalties could be assessed.

(d) COORDINATION BETWEEN FEDERAL AGENCIES AND DEPARTMENTS REGARDING REQUESTS FOR COVERED ACTIVITIES.—Should time permit, a request made by an appropriate issuing authority pursuant to subsection (a)(1) , for a covered entity to engage in covered activity, shall be done in coordination with the appropriate Sector-Specific Agency. If time does not permit such coordination, then the entity issuing the request shall notify the Sector-Specific Agency of the request at the time it is issued.

(e) PROMULGATING REGULATIONS.—Not later than 180 days after the date of the enactment of this Act, the Attorney General, in coordination with the Secretary of Homeland Security and in consultation with the Secretary of Defense and the Secretary of Energy, shall promulgate regulations establishing procedures and criteria for requests or orders for covered activity made pursuant to this Act. In promulgating regulations pursuant to this subsection, the Attorney General shall—

(1) facilitate collaboration and joint action between the public and private sectors;

(2) reserve the authorities of this Act for incidents that threaten or impact national security;

(3) establish mechanisms to ensure an appropriate balance between the need to respond to a national security threat and the importance of protecting the rights and safety of individuals;

(4) provide for flexible and prompt response to address threats and actions by malicious adversaries seeking to harm the national security, economic security, or public health and safety of the United States;

(5) require a covered entity, not later than 24 hours after receiving the request or order, to inform in writing the appropriate issuing authority pursuant to subsection (a)(1) if it is found that there exists a substantial limitation or restriction on the entity's ability to comply with the request or order, the nature of the limitation or restriction, and, as applicable, any proposed changes to the request or order necessary to enable the entity to carry out the covered activity; and

(6) require a covered entity, not later than 90 days after taking any action pursuant to a request or order for a covered action, to provide in writing to the appropriate issuing authority pursuant to subsection (a)(1) a report that outlines—

(A) the entity's implementation of the request or order;

(B) impact of the covered action in meeting the intent or stated objectives of the request or order;

(C) any risks or hazards identified in taking the covered action; and

(D) steps taken to address identified risks and hazards and protect individual rights and public safety.

(f) SAVINGS CLAUSES.—

(1) APPLICABLE LAW.—Nothing in this section affects a public liability action covered by section 170 of the Atomic Energy Act of 1954 (42 U.S.C. 2210).

(2) AVAILABLE DEFENSES.—Nothing in this section undermines or limits the availability of any applicable common law or statutory defense available to a subsection (a)(2) covered entity.

## 3.3.5 Establish a Biennial National Cyber Tabletop Exercise

This legislation would implement the Commission's proposal for the Federal government to conduct a cyber exercise every two years for ten years. As drafted, Federal, State, private sector, and foreign governments could be invited to participate. While the legislation would make the exercises mandatory, it would leave significant flexibility to the executive branch in planning and executing the exercises and determining which agencies, States, industries and foreign partners would be invited to participate.

---

**A BILL**

To establish a national, biennial cyber tabletop exercise including Federal, State, private sector, and foreign participants, and for other purposes.

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

**SEC. 1. BIENNIAL NATIONAL CYBER EXERCISE**

(a) REQUIREMENT.—Not later than December 31, 2023, and not less frequently than once every 2 years thereafter until a date that is not less than 10 years after the date of enactment of this Act, the Secretary, in consultation with the President and the Secretary of Defense, shall conduct an exercise to test the resilience, response, and recovery of the United States in the case of a significant cyber incident impacting critical infrastructure.

(b) PLANNING AND PARTICIPATION.—

(1) IN GENERAL.—Each exercise required under subsection (a) shall be prepared by expert operational planners from—

(A) the Department of Homeland Security;

(B) the Department of Defense;

(C) the Federal Bureau of Investigation; and

(D) appropriate elements of the intelligence community, as specified or designated under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)) identified by the Director of National Intelligence.

(2) ASSISTANCE.—The Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall provide assistance to the expert operational planners described in paragraph (1) in the preparation of each

exercise required under subsection (a).

(c) PARTICIPANTS.—The exercise will include representatives from the Federal government, State governments, and the private sector.

(1) FEDERAL GOVERNMENT PARTICIPANTS.—

(A) Relevant interagency partners, as determined by the Secretary, shall participate in the exercise required under subsection (a), including relevant interagency partners from—

(i) law enforcement agencies;

(ii) elements of the intelligence community, as specified or designated under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)); and

(iii) the Department of Defense.

(B) Senior leader representatives from sector-specific agencies, as determined by the Secretary, shall participate in the exercise required under subsection (a).

(C) Under subparagraph (B), the Secretary shall determine that not less than 1 senior leader representative from each sector-specific agency participates in an exercise required under subsection (a) not less frequently than once every 4 years.

(2) STATE AND LOCAL GOVERNMENTS.—The Secretary shall invite representatives from State, local, and tribal governments to participate in the exercise required under subsection (a) if the Secretary determines the participation of those representatives to be appropriate.

(3) PRIVATE SECTOR.—Depending on the nature of an exercise being conducted under subsection (a), the Secretary, in consultation with the senior leader representative of the sector-specific agencies participating in the exercise under paragraph (1)(B), shall invite the following individuals to participate:

(A) Representatives from private entities.

(B) Other individuals that the Secretary determines will best assist the United States in preparing for, and defending against, a cyber attack;

(4) INTERNATIONAL PARTNERS.—Depending on the nature of an exercise being conducted under subsection (a), the Secretary shall invite allies and partners of the United States to participate in the exercise.

(d) OBSERVERS.—The Secretary may invite representatives from the executive and legislative branches of the Federal government to observe the exercise required under subsection (a).

(e) ELEMENTS.—The exercise required under subsection (a) shall include the following elements:

(1) Exercising of the orchestration of cybersecurity response and the provision of cyber support to Federal, State, local, and tribal governments and private entities, including exercising of the command, control, and deconfliction of operational responses of—

(A) the National Security Council;

(B) interagency coordinating and response groups; and

(C) each Federal government participant described in subsection (c)(1).

(2) Testing of the information-sharing needs and capabilities of exercise participants.

(3) Testing of the relevant policy, guidance, and doctrine, including the National Cyber Incident Response Plan of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security.

(4) A test of the interoperability of Federal, State, local, and tribal governments and private entities.

(5) Exercising of the integration of operational capabilities of the Department of Homeland Security, the Cyber Mission Force, Federal law enforcement agencies, and elements of the intelligence community, as specified or designated under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(6) Exercising of integrated operations, mutual support, and shared situational awareness of the cybersecurity operations centers of the Federal government, including—

(A) the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security;

(B) the Cyber Threat Operations Center of the National Security Agency;

(C) the Joint Operations Center of the United States Cyber Command;

(D) the Cyber Threat Intelligence Integration Center of the Office of the Director of National Intelligence;

(E) the National Cyber Investigative Joint Task Force of the Federal Bureau of Investigation;

(F) the Defense Cyber Crime Center of the Department of Defense; and

(G) the Intelligence Community Security Coordination Center of the Office of the Director of National Intelligence.

(f) BRIEFING.—

(1) IN GENERAL.—assessment of the observed decision and response not later than 180 days after the date on which each exercise required under subsection (a) is conducted, the President shall submit to the appropriate congressional committees a briefing on the participation of the Federal government participants described in subsection (c)(1) in the exercise;

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

(A) an assessment of the decision and response gaps observed in the national level response exercise described in paragraph (1);

(B) proposed recommendations to improve the resilience, response, and recovery of the United States in the case of a significant cyber attack against critical infrastructure;

(C) plans to implement the recommendations described in subparagraph (B); and

(D) specific timelines for the implementation of the plans described in subparagraph (C).

(g) RELATIONSHIP TO OTHER REQUIREMENTS.—Subsection (b) of section 1648 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92; 129 Stat. 1119) is repealed.

(h) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—In this section, 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 Committee on Homeland Security of the House of Representatives; and

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

(2) PRIVATE ENTITY.—In this section the term “private entity” shall have the meaning given such term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

(3) SECRETARY.—The term “Secretary” means the Secretary of Homeland Security.

(4) SECTOR-SPECIFIC AGENCIES.—In this section, the term "Sector-Specific Agencies" has the meaning given such term in section 2201 of the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.).

(5) STATE.— The term “State” means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Northern Mariana Islands, the United States Virgin Islands, Guam, American Samoa, and any other territory or possession of the United States.

## 3.3.6 Clarify National Guard Capabilities

This proposal implements the Commission's recommendation to direct DoD to update existing policies to consider National Guard activities that could be performed and reimbursed under Title 32 of the U.S. Code.

---

**SEC. 1. NATIONAL GUARD.**

To clarify the use of and the role of the National Guard in preparing for, responding to, and recovering from cybersecurity incidents that overwhelm State and local civilian assets, the Secretary of Defense shall—

(a) review and, if necessary, update regulations promulgated under section 903 of title 32, United States Code, to allow the participation of the National Guard in response to a cyberattack as a "homeland defense activity" under section 902 of such title;

(b) direct the Chief of the National Guard Bureau to promulgate guidance on how National Guard units shall collaborate with the Cybersecurity and Infrastructure Security Agency and the Federal Bureau of Investigation through multi-agency task forces, information-sharing groups, incident response planning and exercises, and other relevant forums and activities; and

(c) coordinate with the Secretary of Homeland Security to develop an annex in the National Cyber Incident Response Plan that details the regulations and guidance detailed in subsection (1) and (2) of this Section.

## 3.4.a Restructure the Election Assistance Commission

This amendment implements the Commission's proposal to create a fifth member of the Election Assistance Commission (EAC) with an expertise in cyberattacks as it relates to elections. Under the proposal the fifth member would serve for a limited term, could not serve as chair of the EAC, and could only vote on matters related to the cybersecurity of elections.

---

**A BILL**

To improve the capacity of the Election Assistance Commission to prepare for and respond to cyberattacks on the U.S. election system, and for other purposes.

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

**SEC. 1. ELECTION ASSISTANCE COMMISSION STRUCTURE.**

(a) Section 203 of the Help America Vote Act of 2002 (52 U.S.C. 20923), is amended—

(1) in subsection (a)—

(A) in paragraph (1)—

(i) by striking "four" and inserting "five" after "The Commission shall have";

(ii) by inserting "Of the five Commissioners appointed under this section, one shall be appointed to be the Cybersecurity Commissioner." after "by and with the advice and consent of the Senate."; and

(B) in paragraph (3), by striking "Each member of the Commission shall have experience with or expertise in election administration or the study of elections." And inserting "The Cybersecurity Commissioner shall have expertise in the cybersecurity of electronic voting, electronic voting equipment, or ensuring the cybersecurity of voting. The four other members of the Commission shall have experience with or expertise in election administration or the study of elections.";

(2) in subsection (b)—

(A) in paragraph (1), by striking "(2) and (3)" and inserting "(2), (3) and (4)";

(B) in paragraph (2), by inserting ", other than the Cybersecurity Commissioner," after "of the members";

(C) by adding at the end the following new paragraph:

"(4) TERM OF CYBERSECURITY COMMISSIONER.—The Cybersecurity Commissioner shall serve a term of two years and may be reappointed for not more than two additional terms."; and

(3) in subsection (c), by inserting at the end the following new paragraph:

"(3) LIMITATIONS.

"(A) The Cybersecurity Commissioner shall not serve as chair or vice chair of the Commission.

"(B) The Cybersecurity Commissioner may participate in all Commission proceedings, except that—

"(i) the Cybersecurity Commissioner may vote only on matters that relate to the cybersecurity of elections; and

"(ii) the chair shall determine whether a matter to be voted on relates to the cybersecurity of elections.".

## 3.4.b - Strengthen the Election Assistance Commission

This proposal implements the Commission's recommendation to strengthen and better resource the Election Assistance Commission, particularly with lessons learned in the wake of the COVID-19 Pandemic. The proposal does six things:

- Gives the EAC explicit authority to publicize best practices for the cybersecurity of voting systems and non-voting election systems that are critical for the effective administration of elections;
- Increases the pay of the EAC Commissioners and the maximum allowable staff compensation. The roles and responsibilities of the Commission have increased, increasing Commissioner and staff leadership pay will ensure the best, and most qualified candidates continue to serve the Commission and its staff;
- Adds cyber expertise to the Commission's staff by creating a Senior Cyber Policy Advisor;
- Eliminates the EAC's annual operating budget cap to better enable the EAC in executing its core responsibilities;
- Creates an exemption to the Paperwork Reduction Act removing a significant barrier to quickly gathering and broadly sharing critical information from State and local election officials and others in times of national crisis that may significantly impact elections; and
- Gives the EAC explicit authority to issue grants for research on non-voting election systems.

---

**A BILL**

To amend the Help America Vote Act of 2002 (52 U.S.C. 20901 et seq.) to improve the performance of the Election Assistance Commission of the United States, and for other purposes.

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

**SEC. 1. SHORT TITLE.**

This Act may be cited as the "Strengthening the Election Assistance Commission Act of 2020".

**SEC. 2. DUTIES OF THE COMMISSION**

Section 202 of The Help America Vote Act of 2002 is amended—

(1) in paragraph (5), by striking "; and" and inserting ";";

(2) in paragraph (6), by striking the period at the end; and

(3) by adding at the end the following new paragraph:

"(7) to develop voluntary standards, publicize, educate, and train election officials and others on the cybersecurity best practices for voting technology and non-voting election technology. The Commission may issue best practices as developed by other organizations, such as the National Institute of Standards Technology or the Cybersecurity and Infrastructure Security Agency.".

**SEC. 3. MEMBERSHIP AND APPOINTMENT**

Section 203(d)(1) of the Help America Vote Act of 2002 is amended by striking "level IV of the Executive Schedule under section 5315" and inserting "level II of the Executive Schedule under section 5313 ";

**SEC. 4. STAFF**

Subsection (a) of section 204 of the Help America Vote Act of 2002 (52 U.S.C. 20924) is amended by striking "level V of the Executive Schedule under section 5316" each place it appears and inserting "level III of the Executive Schedule under section 5314 ";

**SEC. 5. STRENGTHENING CYBER PROFICIENCY OF THE COMMISSION STAFF**

Section 204 of the Help America Vote Act of 2002 (52 U.S.C. 20924) is amended—

(1) By redesignating paragraph (5) and (6) as paragraphs (6) and (7) respectively.

(2) By inserting after paragraph (4) the following:

"(5) Senior Cyber Policy Advisor. The Commission shall have a Senior Cyber Policy Advisor, who shall be appointed by the Commission and who shall serve under the Executive Director and who shall be the primary policy advisor to the Commission on matters of cyber security for Federal elections.;" and

**SEC. 6. PROPER RESOURCING OF THE COMMISSION**

Section 210 of the Help America Vote Act of 2002 (52 U.S.C. 20930) is amended—

(1) by striking "for each of the fiscal years 2003 through 2005" and inserting "for fiscal year 2021 and each succeeding fiscal year"; and

(2) by striking "(but not to exceed $10,000,000 for each such year)".

**SEC. 7. IMPROVING THE EFFECTIVENESS OF THE COMMISSION IN AN EMERGENCY OR NATIONAL DISASTER**

(a) In General.—The Help America Vote Act of 2002 (52 U.S.C. 20901 et seq.), is amended by inserting after section 209, the following new section:

**"SEC. 209a. INAPPLICABILITY OF CERTAIN ADMINISTRATIVE PROVISIONS.—**

"(a) In General—In an emergency under subsection (b), the provisions of the Paperwork Reduction Act (44 U.S.C. 3501 et seq.) shall not apply to the activities of the Commission.

"(b) Emergency Criteria.—An emergency under subsection (a) occurs when the majority of the Commission finds that the Paperwork Reduction Act will substantially affect the Commission's ability to accomplish its mission, and—

"(1) there has been a declaration of "emergency" or "major disaster" that meets the definition given such terms in the Disaster Relief Act of 1974 (42 U.S.C. 5122); or

"(2) the Secretary of Homeland Security has declared a cyber state of distress.

"(c) Duration.—An emergency under this section shall, unless renewed by the Commission under subsection (b), extend for the shorter of—

"(1) the duration of the declaration under subsection (b)(1) or (b)(2); or

"(2) thirty days.

"(d) Notice.—Any time the Commission exercises the authority under subsection (a) the Commission shall publish in the Federal Register and on its own website the actions the Commission has taken and the Commission's rationale for that action.".

(b) CLERICAL AMENDMENT.—The table of contents of the Help America Vote Act of 2002 (52 U.S.C. 20901 et seq.) is amended by inserting after the item relating to section 209 the following new item:

"Sec. 209a. Inapplicability of Certain Administrative Provisions.".

**SEC. 8. GRANTS FOR RESEARCH ON VOTING AND NON-VOTING ELECTION TECHNOLOGY IMPROVEMENTS**

Section 271 of the Help American Vote Act of 2002 (52 U.S.C. 21041) is amended—

(1) in the heading, by inserting “and non-voting election” after “voting”; and

(2) in subsection (a), by—

(A) inserting “cybersecurity,” after “and development to improve the quality, reliability, accuracy, accessibility, affordability, ”; and

(B) striking “and voting technology” and inserting “election systems and voting technology.”.

## 3.4.1 Modernize Campaign Regulations to Promote Cybersecurity

Nation-state adversaries have repeatedly attempted to hack U.S. political campaigns for the dual purposes of gathering intelligence and sowing political discord through the selective disclosure of otherwise private, campaign-specific information. Campaign organizations need more cybersecurity resources to protect themselves, but Federal campaign finance law: (1) limits the financial support that national political parties can provide to campaigns, and (2) broadly prohibits corporate contributions to campaigns. In the past two years, the Federal Election Commission has issued several advisory opinions on this issue, but greater statutory clarity and flexibility is needed. As a result, Congress should amend the Federal Election Campaign Act to allow corporations to provide free and reduced-cost cybersecurity assistance to political campaigns on a nonpartisan basis.

---

**SEC. 1. CONTRIBUTIONS OR EXPENDITURES BY NATIONAL BANKS, CORPORATIONS, OR LABOR ORGANIZATIONS.**

Section 316 of the Federal Election Campaign Act of 1971 (52 U.S.C. 30118) is amended in subsection (b)(2), by—

(1) striking "and" before "(C) the establishment, administration, and solicitation of contributions"; and

(2) inserting "; and (D) the provision of free or reduced-cost cybersecurity products or services, as long as such products or services are offered pursuant to nonpartisan and objective criteria, and without regard to political affiliation" after "corporation without capital stock".

## 3.5.a Build Societal Resilience to Foreign Malign Cyber-Enabled Information Operations

The U.S. government should promote digital literacy, civics education, and public awareness to build societal resilience to foreign malign cyber-enabled information operations. Congress should enable the Department of Education by authorizing a grant program funding NGOs, private-sector entities, and SLTT education agencies both to study how best to improve digital citizenship and to incorporate effective digital literacy curricula in American classrooms at the K-12 level and beyond.

---

**A BILL**

To direct the Secretary of Education to establish a program awarding competitive grants for the development of education programs enabling Americans to identify foreign malign cyber-enabled information operations through improved digital literacy, modernized civics education, and broader public awareness.

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

**SEC. 1. SHORT TITLE.**

This Act may be cited as the "Educating Americans on Cyber-Enabled Information Operations Act".

**SEC. 2. PURPOSE.**

The purpose of this Act is to build societal resilience to foreign malign cyber-enabled information operations by promoting public awareness of such operations, improving the public's digital literacy, and strengthening modern civics education.

**SEC. 3. EDUCATION GRANTS PROMOTING THE IDENTIFICATION AND UNDERSTANDING OF FOREIGN MALIGN CYBER-ENABLED INFORMATION OPERATIONS.**

(a) AUTHORIZATION OF GRANTS.—

(1) IN GENERAL.—From the amounts made available to carry out this Act, the Secretary of Education shall establish a program under which the Secretary shall award grants, on a competitive basis, to build societal resilience to foreign malign cyber-enabled information operations by—

(A) helping Americans better identify foreign malign cyber-enabled information operations;

(B) improving the public's digital literacy; and

(C) modernizing civics education, and public awareness. These grants should include both curricula intended for K-12 education, as well as education and public awareness programs for adults.

(2) MAXIMUM GRANT AMOUNT.—A grant awarded under this section may not exceed $500,000.

(b) USE OF FUNDS.—An eligible entity that receives a grant under this section shall use the grant funds to develop and implement education programs intended to help Americans identify foreign malign cyber-enabled information operations by promoting digital literacy, civics education, and public awareness.

(c) APPLICATION.—To be selected 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 information as the Secretary may require. The Secretary shall publish the methodology for assessing grant applications annually, in accordance with the Administrative Procedures Act.

(d) PRIORITY.—In awarding grants under subsection (a), the Secretary shall give priority to candidate programs that—

(1) incorporate critical thinking and problem-solving skills, information on implicit versus explicit messaging, and technology concepts;

(2) leverage the latest and best research on how to improve digital citizenship via digital literacy curricula; and

(3) are designed to work in tandem with existing initiatives being pursued by the Department of Homeland Security and other relevant agencies; and

(4) are consistent with the constitutional protections of free speech.

(e) REPORTING REQUIREMENTS.—An eligible entity recipient under this Act shall annually submit a report to the Secretary that includes a description of how any funds awarded to the eligible entity under this Act have been used during the period covered by the report.

(f) ELIGIBLE ENTITY DEFINED.—In this section, the term "eligible entity" means—

(1) State, local, territorial, and tribal governments' education agencies;

(2) domestic nongovernmental organizations; and

(3) such other U.S.-based domestic entities as the Secretary determines appropriate.

(g) AUTHORIZATION OF APPROPRIATIONS.—For grants under this section, there is authorized to be appropriated $15,000,000 for fiscal year 2021.

## 3.5.b Build More Effective Cybersecurity Awareness Campaigns

Congress should direct the Government Accountability Office (GAO) to study the effectiveness of existing cybersecurity awareness efforts and authorize and fund the Department of Homeland Security (DHS), with support from the National Institute of Standards and Technology (NIST) and the National Science Foundation (NSF), to establish a grant program to support research on the effectiveness of cybersecurity literacy curricula.

---

**A BILL**

To determine how to craft and implement effective cybersecurity awareness campaigns.

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

**SEC. 1. U.S. GOVERNMENT ACCOUNTABILITY OFFICE STUDY.**

Not later than one year after the date of enactment of this Act, the Comptroller General of the United States shall submit to the Homeland Security & Governmental Affairs Committee of the Senate and to the Committee on Homeland Security of the House of Representatives a report that—

(1) addresses, at minimum—

(A) the effectiveness of government spending on cybersecurity awareness efforts to date; and

(B) the effectiveness of the "Stop. Think. Connect." campaign.

**SEC. 2. GRANTS TO STUDY HOW TO BUILD BETTER CAMPAIGNS TO RAISE PUBLIC AWARENESS OF CYBER THREATS AND CYBERSECURITY.**

(a) AUTHORIZATION OF GRANTS.—

(1) IN GENERAL.—The Secretary of the Department of Homeland Security, in coordination with the National Science Foundation and National Institute of Standards and Technology, may provide grants for research and proposals for effective mechanisms to improve, develop, and implement a public awareness and education initiative on cybersecurity.

(2) MAXIMUM GRANT AMOUNT.—A grant awarded under this section may not exceed $500,000.

(b) USE OF FUNDS.—An eligible entity that receives a grant under this section shall use the grant funds to research effective mechanisms to improve, develop, and implement a public awareness and education initiative on cybersecurity.

(c) APPLICATION.—To be selected 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 information as the Secretary may require.

(d) PRIORITY.—In awarding grants under subsection (a), the Secretary shall give priority to candidate programs that research how best to achieve:

(1) Actionable, consistent public messaging on cybersecurity threats and responses with very specific desired outcomes.

(2) Wide propagation of cybersecurity warnings among information technology professionals.

(3) Modern, vetted, and continually updated "train-the-trainer" resources for academic institutions, trade schools, and other organizations seeking to provide cybersecurity education to the public.

(4) Demonstrably effective methods for bringing specific and actionable cyber threat information to the attention of the general public.

(e) ELIGIBLE ENTITY DEFINED.—In this section, the term "eligible entity" means—

(1) State, local, territorial, and tribal governments' education agencies;

(2) nongovernmental organizations;

(3) private-sector entities; or

(4) such other entities as the Secretary determines appropriate.

(f) AUTHORIZATION OF APPROPRIATIONS.—For grants under this section, there is authorized to be appropriated $10,000,000 for fiscal year 2021.

## 3.5.1 Enhance Transparency of Online Political Advertisements as a Defense Against Foreign Influence

This amendment implements the Commission's proposal to amend the Federal Election Campaign Act of 1971 to specifically require that all U.S. online political advertisements be subject to the same restrictions on foreign national purchases as those in place for other traditional mediums. This proposal should be read in consonance with the Commission's additional recommendations to require application of disclaimer statements to online communications and expand the definitions of "electioneering communication" and "public communication," which are already encompassed by legislative proposals currently pending before Congress.

---

**A BILL**

To enhance the transparency of online political advertisements, and for other purposes.

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

**SEC. 1. FEDERAL ELECTION CAMPAIGN ACT OF 1971.**

(a) Section 301 of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101 et seq.) is amended—

(1) in paragraph (8)(B) (v), by inserting ", paid internet or paid digital communication" after "any such listing made on broadcasting stations";

(2) in paragraph (9)(B)—

(A) in clause (i), by—

(i) inserting "or any print, online, or digital" after "broadcasting station", inserting "blog, publication," after "magazine"; and

(ii) inserting "broadcasting, print, online, or digital-" before "facilities are owned or controlled"; and

(B) in clause (iv), by inserting "paid internet or paid digital communication," after "or in newspapers, magazines"; and

(3) in paragraph (22), by inserting "paid internet or paid digital" after "broadcast, cable", or "satellite".

(b) Section 103(b)(1) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101 et seq.) in paragraph (8)(B) is amended —

(1) in clause (ix), by inserting "paid internet or paid digital communication," after "direct mail,"; and

(2) in clause (x), by inserting "paid internet or paid digital communication," after "direct mail,";

(c) Section 304 of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101 et seq.) is amended—

(1) in paragraph (3)(A)(i), by—

(A) inserting ", or qualified internet or digital" before "communication which—"; and

(B) striking "a" after "in the case of" and inserting "any broadcast, cable or satellite" before "communication which refers to a candidate for an office other than President or Vice President";

(2) in paragraph (3)(A)(ii),by inserting ", or qualified internet or digital" after ""any broadcast, cable or satellite";

(3) in paragraph (3)(B)(i), by—

(A) inserting "or any online or digital newspaper, magazine, blog, publication, or periodical," after "the facilities of any broadcasting station,"; and

(B) inserting "broadcasting, online, or digital" after "unless such"; and

(4) by adding at the end of paragraph (3) the following new subparagraphs:

"(D) QUALIFIED INTERNET OR DIGITAL COMMUNICATION.—The term 'qualified internet or digital communication' means any communication which is placed or promoted for a fee on an online platform.

"(E) ONLINE PLATFORM.—For purposes of this subsection, the term 'online platform' means any public-facing website, web application, or digital application (including a social network, ad network, or search engine) which—

"(i) sells qualified political advertisements; and

"(ii) has 25,000,000 or more unique monthly United States visitors or users for a majority of months during the preceding 12 months.

"(F) QUALIFIED POLITICAL ADVERTISEMENT.—

"(i) IN GENERAL.— For purposes of this subsection, the term 'qualified political advertisement' means any advertisement (including search engine marketing, display advertisements, video advertisements, native advertisements, and sponsorships) that—

"(I) is made by or on behalf of a candidate; or

"(II) communicates a message relating to any political matter of national importance, including—

"(aa) a candidate;

"(bb) any election Federal office; or

"(cc) a national legislative issue of public importance.".

(d) Section 318 of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101 et seq.), is amended—

(1) in subsection (a)—

(A) by inserting "paid internet or paid digital communication," before "or any other type of general public political advertising, or whenever any person makes a disbursement";

(B) by inserting "paid internet or paid digital communication," before "or any other type of general public political advertising, or any other type of general public political advertising or makes a disbursement for an electioneering communication";

(C) in paragraph (1), by striking "clearly state" and inserting "state in a clear and conspicuous manner";

(D) in paragraph (2), by striking "clearly state" and inserting "state in a clear and conspicuous manner"; and

(E) by inserting at the end the following flush sentence:

"For purposes of this subsection, a communication does not make a statement in a clear and conspicuous manner if it is difficult to read or hear or if the placement is easily overlooked.";

(2) in subsection (d)—

(A) in paragraph (1)(A)—

(i) by striking "By radio" and inserting "Audio Format"; and

(ii) by striking "transmitted through radio" and inserting "in an audio format";

(B) in paragraph (1)(B)—

(i) by striking "By television" and inserting "Video Format"; and

(ii) by striking "transmitted through television" and inserting "in video format"; and

(C) in paragraph (2)—

(i) by striking "transmitted through radio or television" and inserting "made in audio or video format"; and

(ii) by striking "through television" and inserting "in video format"; and

(3) by inserting at the end the following new subsections:

"(e) SPECIAL RULES QUALIFIED INTERNET OR DIGITAL COMMUNICATIONS.—

"(1) SPECIAL RULES WITH RESPECT TO STATEMENTS.—In the case of any qualified internet or digital communication (as defined in section 304(f)(3)(D)) which is disseminated through a medium in which the provision of all of the information specified in this section is not practicable, the communication shall, in a clear and conspicuous manner—

"(A) state the name of the person who paid for the communication; and

"(B) provide a means for the recipient of the communication to obtain the remainder of the information required

under this section with minimal effort and without receiving or viewing any additional material other than such required information.

"(2) SAFE HARBOR FOR DETERMINING CLEAR AND CONSPICUOUS MANNER.—A statement in qualified internet or digital communication (as defined in section 304(f)(3)(D)) shall be considered to be made in a clear and conspicuous manner as provided in subsection (a) if the communication meets the following requirements:

"(A) TEXT OR GRAPHIC COMMUNICATIONS.— In the case of a text or graphic communication, the statement—

"(i) appears in letters at least as large as the majority of the text in the communication; and

"(ii) meets the requirements of paragraphs (2) and (3) of subsection (c).

"(B) AUDIO COMMUNICATIONS.—In the case of an audio communication, the statement is spoken in a clearly audible and intelligible manner at the beginning or end of the communication and lasts at least three seconds.

"(C) VIDEO COMMUNICATIONS.—In the case of a video communication which also includes audio, the statement—

"(i) is included at either the beginning or the end of the communication; and

"(ii) is made in both—

"(I) a written format that meets the requirements of subparagraph (A) and appears for at least 4 seconds; and

"(II) an audible format that meets the requirements of subparagraph (B).

"(D) OTHER COMMUNICATIONS.—In the case of any other type of communication, the statement is at least as clear and conspicuous as the statement specified in subparagraphs (A), (B), or (C).

"(3) NONAPPLICATION OF CERTAIN EXCEPTIONS.—The exceptions provided in section 22110.11(f)(1)(i) and (ii) of title 11, Code of Federal Regulations, or any successor to such rules, shall have no application to qualified internet or digital communications (as defined in section 304(f)(3)(D) of this Act).".

## 4.1 Establish a National Cybersecurity Certification and Labeling Authority

This proposal implements the Commission's recommendation to create a National Cybersecurity Certification and Labeling Authority to establish and manage a voluntary cybersecurity certification and labeling program for information and communication technologies.

---

**A BILL**

To establish a National Cybersecurity Certification and Labeling Authority, and for other purposes.

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

**SEC. 1. DEFINITIONS.**

In this Act:

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

(2) CERTIFICATION.—The term "certification" means a seal or symbol provided by the National Cybersecurity Certification and Labeling 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.

(3) 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 national critical functions as determined by the Department of Homeland Security.

(4) 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

**SEC. 2. NATIONAL CYBERSECURITY CERTIFICATION AND LABELING AUTHORITY.**

(a) ESTABLISHMENT.—There is established a National Cybersecurity Certification and Labeling Authority (hereinafter referred to as "NCCLA") for the purpose of administering a voluntary cybersecurity certification and labeling program for critical information and communications technologies.

(b) PROGRAMS.—

(1) ACCREDITATION OF CERTIFYING AGENTS.—The NCCLA shall define and publish a process whereby non-governmental entities may apply to become accredited certifying agents for specific critical information and communications technologies.

(2) IDENTIFICATION OF STANDARDS, FRAMEWORKS, AND BENCHMARKS.—The Authority shall work in close coordination with the Department of Commerce, the Department of Homeland Security, and subject matter experts from the Federal government, academia, non-governmental 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.

(3) PRODUCT CERTIFICATION.—The Authority, in consultation with the Department of Commerce, the Department of Homeland Security, and other experts from the Federal government, academia, non-governmental organizations, and the private sector, shall—

(A) 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;

(B) 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 pursuant to paragraph (2) of this subsection;

(C) issue, or permit accredited certifying agents to issue, certifications for products and services that meet and comply with security standards, frameworks, and benchmarks endorsed by the Authority through the work conducted under title (e)(3)(b) of this statute;

(D) permit a manufacturer or distributor of a covered product to display a certificate reflecting the extent to which the covered product meets established and identified cybersecurity and data security benchmarks;

(E) remove the certification of a covered product as a covered product certified under the program if the manufacturer of the certified covered product falls out of conformity with the benchmarks established under paragraph (e)(2) for the covered product;

(F) work to enhance public awareness of the Authority's certificates and labeling, including through public outreach, education, research and development, and other means; and

(G) publicly display a list of certified products, along with their respective certification information.

(4) CERTIFICATIONS.—

(A) IN GENERAL.—Certifications granted pursuant to this Act shall remain valid for one year from the date of issuance.

(B) CLASSES OF CERTIFICATION.—In developing the guidelines and criteria required pursuant to paragraph (3), the Authority shall designate at least three classes of certifications, including:

(i) For products and services that product manufacturers and service providers of critical information and communications attest meet the criteria for a certification, Attestation-based Certification.

(ii) For products that have undergone a security evaluation and testing process by a qualifying third party, Accreditation-based Certification.

(iii) For products that have undergone a security evaluation and testing process by a qualifying third party, Test-based Certification.

(5) PRODUCT LABELING.—The Authority, in consultation with the Department of Commerce, the Department of Homeland Security, and other experts from the Federal government, academia, non-governmental organizations, and the private sector, shall—

(A) 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

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

(c) ENFORCEMENT.—The Federal Trade Commission shall set and levy fines under Section 5(a) of the Federal Trade Commission Act (FTC Act) (15 USC §45) if it is found that a product manufacturer, distributor, or seller has—

(1) falsely attested to, or has falsified an audit or test for, a security standard, framework, or benchmark for certification;

(2) intentionally mislabeled products; or

(3) has failed to maintain the security standard, framework, or benchmark to which they have attested.

**SEC. 3. SELECTION OF THE AUTHORITY.**

(a) SELECTION.—The Secretary of Commerce, in coordination with the Secretary of Homeland Security, shall issue a notice of funding opportunity and select, on a competitive basis, a non-profit, non-governmental organization to serve as the National Cybersecurity Certification and Labeling Authority (hereafter referred to as 'NCCLA') for period of 5 years.

(b) ELIGIBILITY FOR SELECTION.—The Secretary of Commerce may only select an organization to serve as the NCCLA if such organization—

(1) is a nongovernmental, not-for-profit, 501(c)3 designated organization;

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

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

(c) APPLICATION.—The Secretary of Commerce shall establish a process by which a non-profit, non-governmental organization that seeks to be selected as the NCCLA may apply for consideration.

(d) PROGRAM EVALUATION.—Not later than the date that is four years after the initial selection pursuant subsection (a), and every four years thereafter, the Secretary of Commerce, in consultation with the Secretary of Homeland Security, shall—

(1) assess the effectiveness of the labels and certificates produced by the NCCLA, including—

(A) assessing the costs to businesses that manufacture covered products participating in the Authority's program;

(B) evaluating the level of participation in the NCCLA's program by businesses that manufacture covered products;

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

(2) audit the impartiality and fairness of the NCCLA's activities conducted pursuant to section 2 of this Act;

(3) issue a public report on the assessment required pursuant to paragraph (1) and (2); and

(4) brief Congress on the findings of the assessment and report required by this subsection.

(e) RENEWAL.—After the initial selection pursuant to subsection (a), the Secretary of Commerce, in consultation with the Secretary of Homeland Security, shall, every five years—

(1) accept applications from non-profit, non-governmental organizations seeking selection as the NCCLA; and

(2) following competitive consideration of all applications—

(A) renew the selection of the existing NCCLA; or

(B) select another applicant organization to serve as the NCCLA.

## SEC. 4. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated such sums as may be necessary to carry out this Act. Such funds shall remain available until expended.

## 4.1.1 Designate Critical Technology Security Centers

This proposal should direct and appropriate funds for the Department of Homeland Security to competitively select, designate, and fund up to three Critical Technology Security Centers in order to centralize efforts directed toward evaluating and testing the security of devices and technologies that underpin our networks and critical infrastructure.

---

**SEC. 1. DEPARTMENT OF HOMELAND SECURITY CRITICAL TECHNOLOGY SECURITY CENTERS.**

(a) Section 307 of the Homeland Security Act of 2002, is amended—

(1) In paragraph (b)(3)—

(A) By inserting "national laboratories" before ", and universities";

(B) By inserting at the end the following new subparagraph:

"(E) establish at least one, and up to three, cybersecurity-focused critical technology security center(s) to perform the following functions—

"(i) Network Technology Security, to test the security of cyber-related hardware and software;

"(ii) Connected Industrial Control System Security, to test the security of connected programmable data logic controllers, supervisory control and data acquisition servers, and other cyber connected industrial equipment; and

"(iii) Open Source Software Security, to test and fix vulnerabilities in open-source software repositories.".

## 4.2 Establish Liability for Final Goods Assemblers

This proposal implements the Commission's recommendation to create Federal tort liability for final goods assemblers.

---

**A BILL**

To create Federal tort liability for final goods assemblers, and for other purposes.

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

**SEC. 1. DEFINITIONS.**

In this Act:

(1) COVERED INFORMATION TECHNOLOGY PRODUCT.—The term "covered information technology product" means a device intended for commercial or consumer use that runs firmware and native software; a device intended for commercial or consumer use that runs firmware, native software, and third-party software; and software intended for commercial or consumer use, but shall not include any product that—

(A) is created without mechanisms for monetization; or

(B) has exceeded its stated end of life date and is no longer actively supported for other purposes such as usability improvements or bug fixes;

(C) has received a security patch beyond its stated end of life date.

(2) COVERED SECURITY VULNERABILITY.—The term "covered security vulnerability" means any security vulnerability, unless the vulnerability—

(A) has not been disclosed through existing public databases, such as the National Vulnerability Database, and including, but not limited to being assigned a Common Vulnerabilities and Exposures number;

(B) has not been reported to the final goods assembler by a third party; and

(C) is unknown to the final goods assembler.

(3) CYBERSECURITY INCIDENT.—The term "cybersecurity incident" has the meaning given that term in section 2209 of The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.).

(4) INFORMATION TECHNOLOGY PRODUCT.—The term "information technology product" means an information technology good for or intended for consumer or commercial use.

(5) FINAL GOODS ASSEMBLER.—The term "final goods assembler" means a legal entity that produces, for use in the commercial or consumer context, a covered information technology product.

(6) QUALIFIED EXPERT.—The term "qualified expert" means someone who possesses scientific, technical, or other specialized knowledge regarding the covered information technology product at issue or similar products.

(7) SECURITY PATCH.—The term "security patch" means a software component that, when installed, directly modifies files or device settings related to a different software component.

(8) SECURITY VULNERABILITY.—The term "security vulnerability" has the meaning given that term in the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

(9) SECURITY VULNERABILITY DISCLOSURE.—The term "security vulnerability disclosure" means the process through which an entity discloses information about security vulnerabilities in their information technology products.

(10) SECURITY VULNERABILITY DISCLOSURE POLICY.—The term "security vulnerability disclosure policy" means policies and procedures that govern the process for reporting and disclosing security vulnerabilities in information technology products.

(11) Security Vulnerability Management Program.—The term "security vulnerability management program" means an internal program that establishes a technical process to identify, prioritize, investigate, remediate, and disclose security vulnerabilities that are reported to or discovered by the final goods assembler. A vulnerability management program possesses three primary elements—

(A) a website or portal where the company or its vendor can receive vulnerability information directly from researchers;

(B) a back-end process flow that dictates how a given vulnerability will be validated and, if necessary, remediated; and

(C) an internal governance framework that supports the program and addresses issues related to change controls, management oversight, escalation procedures, and guidelines for external communication.

(12) SECURITY VULNERABILITY REPORTING.—The term "security vulnerability reporting" means the process through which security vulnerabilities may be communicated to the entity responsible for the maintenance of an information technology product in which the security vulnerability was discovered.

## SEC. 2. CREATION OF A PRIVATE RIGHT OF ACTION.

(a) IN GENERAL.—Any end user of a covered information technology product for which the final goods assembler does not meet the standard of care, as established by section 3 who incurs qualifying harms due to a cyber incident caused or enabled by a covered security vulnerability in such covered information technology product may bring a private right of action, to be heard in the U.S. District Court of jurisdiction, against the final goods assembler of the covered information technology product.

(b) RECOVERY.—Subject to the limitation set forth in subsection (c), in a suit brought pursuant to subsection (a), an end user may recover for—

(1) damages suffered;

(2) court costs; and

(3) reasonable attorneys fees and expenses.

(c) LIMITATION.—Notwithstanding the actual amount of damages incurred by an entity which suffers a qualifying harm, damages awarded pursuant to subsection (b)(1) may not exceed 15% of the annual revenue of the preceding year of any entity found liable in a suit brought pursuant to subsection (a).

## SEC. 3. STANDARD OF CARE.

A final goods assembler of a covered information technology product shall, within 18 months of the enactment of this Act, be deemed to meet the standard of care for the purposes of a suit brought pursuant to section 2, if the final goods assembler makes security patches for security vulnerabilities in a covered information technology product available to the public within 90 days of a vulnerability—

(a) being disclosed through existing public databases, such as the National Vulnerability Database, and including, but not limited to, being assigned a Common Vulnerabilities and Exposures number;

(b) being reported to the final goods assembler by a third party; or

(c) being discovered by the final goods assembler.

## SEC. 4. DETERMINATION OF HARM.

(a) QUALIFYING HARMS.—Qualifying harms subject to the private right of action established by section 2 shall include any of the following:

(1) Demonstrable economic loss exceeding $75,000, including through any harm to, or arising from impairment of, the confidentiality, integrity, or availability of data, a program, a system, or information.

(2) Physical damage or destruction.

(3) Physical harm to human safety, security, or loss of life.

(b) CAUSALITY AND ENABLEMENT.—A covered security vulnerability shall be deemed to have caused or enabled a cyber incident if the covered security vulnerability was a substantial factor in bringing about a cybersecurity incident resulting in a qualifying harm.

## SEC. 5. PROCEDURAL REQUIREMENTS.

(a) REQUIREMENT FOR A CERTIFICATE OF MERIT.—In a suit brought pursuant to section 2, the plaintiff shall file an affidavit. Such affidavit shall declare that—

(1) the affiant has consulted and reviewed the facts of the alleged cybersecurity incident with a qualified expert; and

(2) the qualified expert has completed a written report, after examination of the product or a review of literature pertaining to the product.

(b) REPORT REQUIREMENTS.—A report submitted in accordance with subsection (a) shall—

(1) identify specific security vulnerabilities in the product that caused or enabled a cyber incident resulting in a qualifying harm; and

(2) contain a determination that the final goods assembler did not meet the standard of care established in section 3 of this Act for the relevant covered information technology product.

(c) REPORT SUBMISSION.—A copy of the written report submitted in accordance with subsection (a) shall be attached to the original complaint and shall include the name and address of the expert.

(d) SEPARATE REPORT.—A separate report shall be filed for each covered information technology product alleged to have caused or enabled a cyber incident resulting in a qualifying harm.

(e) GROUNDS FOR DISMISSAL.—The failure to file an affidavit as required by subsection (a) shall be grounds for dismissal.

## SEC. 6. REQUIREMENTS FOR FINAL GOODS ASSEMBLERS.

A final goods assembler of a covered information technology product shall, within six months of the enactment of this Act, establish—

(a) a regularly updated security vulnerability disclosure policy, posted on a public website;

(b) a method for the public or independent security researchers to submit security vulnerabilities to the final goods assembler, maintained on a public website; and

(c) an internal security vulnerability management program.

## SEC. 7. ENFORCEMENT BY THE FEDERAL TRADE COMMISSION

(a) ENFORCEMENT—Section 6 of this Act shall be enforced by the Federal Trade Commission in the same manner, by the same means, and with the same jurisdiction as though all applicable terms of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act.

(b) VIOLATION TREATED AS UNFAIR OR DECEPTIVE ACT OR PRACTICE.—A violation of section 6 of this Act shall be treated as an unfair and deceptive act or practice proscribed under a rule issued under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

## 4.3 Establish a Bureau of Cyber Statistics

This proposal establishes a Bureau of Cyber Statistics that would act as the government statistical agency that collects, processes, analyzes, and disseminates essential statistical data on cybersecurity, cyber incidents, and the cyber ecosystem to the American public, Congress, other Federal agencies, State and local governments, and the private sector.

---

**A BILL**

To establish a Bureau of Cyber Statistics to collect, process, analyze, and disseminate essential statistical data on cybersecurity, cyber incidents, and the cyber ecosystem to the American public, Congress, other Federal agencies, State and local governments, and the private sector, and for other purposes.

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

**SEC. 1. SHORT TITLE.**

This Act may be cited as the "Bureau of Cyber Statistics Act"

**SEC. 2. BUREAU OF CYBER STATISTICS.**

(a) ESTABLISHMENT.—There is established within the Department of Commerce a Bureau of Cyber Statistics (hereinafter referred to in this subchapter as "Bureau").

(b) DIRECTOR.—

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

(A) report to the Secretary of Commerce; 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; and

(C) protect against improper or illegal use or disclosure, 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.

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

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

(2) 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;

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

(4) 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 chapter;

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

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

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

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

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

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

(d) FURNISHING 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)(10) shall provide to the Bureau such information as the Director determines necessary to carry out the purposes of this section.

(e) 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 the provisions of 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 contain the in 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 clause subsection (d) and (f).

(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.

(f) PRIVATE SECTOR SUBMISSION OF DATA.—

(1) STANDARDS FOR SUBMISSION OF INFORMATION.—Not later than two years after the enactment of this act, to enable submission of data related to cyber incidents by private entities, the Director shall work with relevant stakeholders to develop submission criteria and standardized procedures.

(2) PRIVATE SECTOR SUBMISSION.—Following the development of the standards required pursuant to paragraph (1), the Director shall publish the processes for submission of data related to cyber incidents and shall begin accepting such submissions.

(3) REPORT.—Not later than one year following than commencement of the submissions pursuant to paragraph (2), the Director shall submit a report to Congress detailing the rate of submissions by private sector entities, an assessment of the procedures for submissions, and an overview of mechanisms for ensuring the collection of data related to cyber incidents from private entities that collect and retain such data as part of their core business activity.

(g) DEFINITIONS.—In this section, "statistical purpose" means—

(1) the description, estimation, or analysis of the characteristics of groups, without identifying the individuals or organizations that comprise such groups; and

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

## SEC. 3. CONFORMING AMENDMENT.

Subchapter II of chapter 53 of title 5, United States Code, is amended in section 5315 by inserting after "Director, Bureau of the Census, Department of Commerce." the following:

"Director, Bureau of Cyber Statistics, Department of Commerce.".

## 4.4 Establish a Cyber Insurance Certification Program at an FFRDC

This proposal implements the Commission's recommendation to resource and direct the Department of Homeland Security to fund a Federally funded research and development center (FFRDC) to work with State-level regulators in developing certifications for cybersecurity insurance products. These voluntary certifications will include underwriter training, claims adjuster training, and cyber insurance product certifications.

---

**A BILL**

To establish a program to develop certifications for cybersecurity insurance products, and for other purposes.

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

**SEC. 1. ESTABLISHMENT OF PROGRAM TO CREATE VOLUNTARY CYBERSECURITY INSURANCE CERTIFICATIONS.**

(a) ESTABLISHMENT.—The Secretary of Homeland Security shall competitively select a not-for-profit, non-governmental organization to establish a program to certify voluntary cybersecurity insurance training and products (hereafter referred to as 'Program').

(b) REQUIREMENTS OF THE PROGRAM.—The Program shall:

(1) Operate for not less than five years, and may be extended in two-year increments upon a determination by the Secretary of Homeland Security that the program has not yet met its purpose.

(2) Be voluntary for all persons and individuals.

(3) Develop, after collaboration with insurers, State regulators, and cybersecurity risk managers, a curriculum and training courses for cyber insurance underwriters required under a cyber insurance underwriter certification.

(4) Issue a certification for any cyber insurance underwriter who meets the standards established in the curriculum and training pursuant to (b)(3) of this Section.

(5) Develop, after collaboration with insurers, State regulators, and cybersecurity risk managers, curriculum and training courses for cyber claims adjusters.

(6) Issue a certification for any cyber claims adjuster that meets the standards established in the curriculum and training pursuant to (b)(5) of this Section.

(7) Develop, in collaboration with State insurance regulators and the public-private working group modeling cyber risk to develop cybersecurity product certifications based on a common lexicon and security standards.

(8) Certify that insurers that voluntarily seek certification for their products meet the standards established in the curriculum and training pursuant to (b)(7) of this Section.

(c) EVALUATION OF CURRICULUM, TRAINING COURSES, AND CERTIFICATES.—The Secretary of Homeland Security, in consultation with other relevant Federal departments, agencies, and private sector stakeholders, shall assess the effectiveness of the curriculum, training courses, and certificates produced by the Program.

(d) FEES FOR TRAINING AND CERTIFICATION.—The program may charge reasonable fees for training and certification.

## 4.4.4 Amend the Sarbanes-Oxley Act to Include Cybersecurity Reporting Requirements and Require Regular Pen Testing

This proposal harmonizes and clarifies cybersecurity oversight and reporting requirements for publicly traded companies by amending the Sarbanes-Oxley Act to explicitly account for cybersecurity and require Pen Testing.

---

**A BILL**

To harmonize and clarify cybersecurity oversight and reporting requirements for publicly traded companies, and for other purposes.

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

**SEC. 1. DEFINITIONS.**

(a) IN GENERAL.—Section 2 of the Sarbanes-Oxley Act of 2002 (15 U.S.C. 7201), is amended by inserting at the end the following:

"(18) CRITICAL INFORMATION SYSTEM.—The term "critical information system" means a set of activities, involving people, processes, data, or technology, which enable the issuer to obtain, generate, use, and communicate transactions and information in pursuit of core business objectives.

"(19) INFORMATION SECURITY CONTROL.—The term "information security control" means a safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

"(20) CYBERSECURITY RISK.—The term "cybersecurity risk" means a significant vulnerability to, or a significant deficiency in, the security and defense activities of an information system.".

**SEC. 2 CORPORATE RESPONSIBILITY FOR FINANCIAL REPORTS AND CRITICAL INFORMATION SYSTEMS**

(a) IN GENERAL.—Section 302 of the Sarbanes-Oxley Act of 2002 (15 U.S.C. 7241) is amended—

(1) in the section heading, by inserting “and critical information systems” after “reports”;

(2) in subsection (a)—

(A) by inserting “and the principal security, risk, or information security officer or officers” after “the principal financial officer or officers”;

(B) in paragraph (4)(A), by inserting “, including information security controls” after “internal controls”;

(C) in paragraph (4)(B), by inserting “, including information security controls” after “internal controls”;

(D) in paragraph (4)(C), by inserting “, including information security controls” after “internal controls”;

(E) in paragraph (4)(D), by inserting “, including information security controls” after “internal controls”;

(F) in paragraph (5)(A), by inserting “and any significant cybersecurity risks in issuer's critical information systems” after “internal controls”; and

(G) in paragraph (6)—

(i) by inserting “, including information security controls” after “significant changes in internal controls”;

(ii) by inserting “, including information security controls” after “could significantly affect internal controls”; and

(iii) by inserting “cybersecurity risks,” before “significant deficiencies”.

(b) CLERICAL AMENDMENT.—

(1) The table of contents of the Sarbanes-Oxley Act of 2002 (15 U.S.C. 7201) is amended by striking the item relating to section 302 and inserting the following new item:

“302. Corporate responsibility for financial reports and critical information systems.”.

**SEC. 3. MANAGEMENT ASSESSMENTS OF INTERNAL CONTROLS AND CRITICAL INFORMATION SYSTEMS.**

(a) IN GENERAL.—Section 404 of the Sarbanes-Oxley Act of 2002 (15 U.S.C. 7241) is amended—

(1) in the section heading, by inserting "and critical information systems" after "controls";

(2) in subsection (a)—

(A) by redesignating paragraph (2) as paragraph (3);

(B) by inserting after paragraph (1) the following new paragraph (2);

"(2) state the responsibility of management for establishing and maintaining adequate internal information security controls, to include penetration testing, as applicable."; and

(C) in paragraph (3), as so redesignated by striking "of the issuer for financial reporting" and inserting "for financial reporting and the internal information security controls of the issuer";

(3) by redesignating subsection (c) as subsection (d);

(4) by inserting after subsection (b) the following new subsection (c):

"(c) Information security control evaluation and reporting. With respect to the internal information security control assessment required by subsection (a), any third-party information security firm that prepares or issues a cyber or information security risk assessment for the issuer, other than an issuer that is an emerging growth company (as defined in section 78c of this title), shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.";

(5) in subsection (d), by striking "Subsection (b)" and inserting "Subsections (b) and (c)";

(6) by inserting after subsection (d) the following new subsection (e):

"(e) Guidance on information security reporting. The Commission shall issue guidance on how to describe information security issues in a way that does not compromise the reporting entity's security controls."

(b) CLERICAL AMENDMENT.—The table of contents of the Sarbanes-Oxley Act of 2002 (15 U.S.C. 7241) is amended by striking the item relating to section 404 and inserting the following new item:

"404. Management assessment of internal controls and critical information systems."

## 4.5 Create a Secure Cloud Certification

This proposal requires the Department of Homeland Security, in consultation with the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB), to work with the National Cybersecurity Certification and Labeling Authority (NCCLA) (separate recommendation (4.1)) to develop a secure cloud certification. If the NCCLA does not exist, DHS would lead the effort with NIST and OMB.

---

**A BILL**

To develop a secure cloud certification, and for other purposes.

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

**SEC. 1. SHORT TITLE.**

This Act may be cited as the "Cloud Security Certification Program".

**SEC. 2. ESTABLISHMENT OF THE CLOUD SECURITY CERTIFICATION PROGRAM.**

There is established a Cloud Security Certification Program within the [National Cybersecurity Certification and Labeling Authority] OR [Department of Homeland Security] to create a voluntary standard for use in certifying a cloud service offered by an eligible entity based on cybersecurity standards developed or recognized by this program.

**SEC. 3. CLOUD SECURITY CERTIFICATION AND METRICS.**

(a) DEVELOPMENT OF CERTIFICATION.—The National Institute of Standards and Technology, in coordination with the [National Cybersecurity Certification and Labeling Authority and the Department of Homeland Security] OR [Department of Homeland Security] shall lead a public-private standards-making process that includes representatives from cloud service providers, as well as private entities from a variety of sectors, to develop a secure cloud standard and certification process.

(b) DEVELOPMENT OF METRICS.—The [National Cybersecurity Certification and Labeling Authority] OR [Department of Homeland Security] shall coordinate with the National Institute of Standards and Technology to develop metrics by which cloud services can be compared and certified based on security.

(c) DURATION.—Any certification given to an eligible entity pursuant to a process developed under this section shall last for no more than two years.

**SEC. 4. CERTIFYING AGENT.**

(a) ESTABLISHMENT OF CERTIFYING AGENT.—[The National Cybersecurity Certification and Labeling Authority shall serve as the certifying agent for the certification established in Section 3] OR [The Department of Homeland Security, in consultation with the National Institute of Standards and Technology, shall serve as the certifying agent for the certification established in Section 3].

(b) REQUIREMENTS.—The Certifying Agent established in subsection (a) of this section shall conduct initial and subsequent audits of eligible entities that apply for and meet the requirements for the certification established in Section 3.

**SEC. 5. UPDATING THE FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM.**

Not later than five years following the date of enactment of this Act, the Director for the Office of Management and Budget shall—

(1) evaluate the feasibility and value of incorporating the cloud security certification and standards developed pursuant to this Act as a requirement under the Federal Risk and Authorization Management Program;

(2) update the requirements of the Federal Risk and Authorization Management Program, as appropriate; and

(3) submit a report to Congress detailing the evaluation undertaken pursuant to paragraph (1) and explaining the basis for any action or inaction pursuant to paragraph (2).

**SEC. 6. ELIGIBLE ENTITY.—** In this section**,** the term "eligible entity" means any cloud service provider or entity that operates cloud services, with a focus on entities that provide infrastructure as a service and platform as a service.

## 4.5.1 Incentivize the Uptake of Secure Cloud Services

This proposal directs the Department of Commerce, Small Business Administration, and the Department of Homeland Security to conduct a six-month study to define the method of incentivizing the adoption of these services, and report their findings and recommendations to Congress.

---

**A BILL**

To incentivize the uptake of secure cloud services, and for other purposes.

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

**SEC. 1. A REPORT ON INCENTIVIZING THE UPTAKE OF SECURE CLOUD SERVICES FOR SMALL AND MEDIUM-SIZED BUSINESSES AND STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS.**

(a) IN GENERAL.—Not later than six months after enactment of this Act, the Secretary of Commerce, in coordination with the Director of the Small Business Administration and the Secretary of Homeland Security, shall conduct a study to propose and review methods of incentivizing the adoption of secure cloud services by small and medium sized businesses and State, local, tribal and territorial governments, and report their findings and recommendations to Congress.

(b) REQUIREMENT.—The report required by subsection (a) shall—

(1) identify barriers or challenges for small and medium-sized businesses and State, local, tribal, and territorial governments in purchasing or acquiring secure cloud services;

(2) assess market availability, market pricing, and affordability for small and medium-sized businesses and State, local, tribal, and territorial governments, with particular attention in identifying high-risk and underserved sectors or regions; and

(3) estimate the timeline and cost of tax breaks for small and medium-sized businesses and grants for State, local, tribal, and territorial governments necessary to incentivize the adoption of secure cloud services.

## 4.5.2 Develop a Strategy to Secure Foundational Internet Protocols and Email

This proposal requires the National Telecommunications and Information Administration and the Department of Homeland Security to develop a strategy and recommendations, in consultation with internet service providers and civil society and academic experts, to define common, implementable guidance for securing Domain Name System, Border Gateway Protocol, and e-mail.

---

**A BILL**

To develop a strategy to secure foundational internet protocols and email, and for other purposes.

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

**SEC. 1. DEVELOP A STRATEGY TO SECURE FOUNDATIONAL INTERNET PROTOCOLS AND EMAIL.**

(a) CREATION OF A STRATEGY TO SECURE FOUNDATIONAL INTERNET PROTOCOLS AND EMAIL.—In order to secure foundational internet protocols and email:

(1) PROTOCOL SECURITY STRATEGY.—The National Telecommunications and Information Administration and the Department of Homeland Security shall not later than December 31, 2021 deliver to Congress a strategy to secure the Border Gateway Protocol and the Domain Name System.

(A) STRATEGY REQUIREMENTS.—The strategy required by paragraph (1) shall—

(i) articulate the security and privacy benefits of implementing Border Gateway Protocol and Domain Name System security as well as the burdens of implementation and the entities on whom those burdens will most likely fall.

(ii) identify key U.S. and international stakeholders.

(iii) outline identified security measures that could be used to secure or provide authentication for the Border Gateway Protocol and the Domain Name System.

(iv) identify any barriers to implementing Border Gateway Protocol and Domain Name System security at scale.

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

(vi) provide an initial estimate of the total cost to government and implementing entities in the private sector of implementing Border Gateway Protocol and Domain Name System security and propose recommendations for defraying these costs, if applicable.

(B) CONSULTATION.—In developing the strategy pursuant to 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 non-profits, and academic experts.

(2) DMARC STRATEGY.—The Department of Homeland Security shall not later than December 31, 2021 deliver to Congress a strategy to implement Domain-based Message Authentication, Reporting, and Conformance standard across all U.S.-based email providers.

(A) REPORT REQUIREMENTS.—The strategy required by paragraph (2) shall—

(i) articulate the security and privacy benefits of implementing the Domain-based Message Authentication, Reporting, and Conformance standard at scale, as well as the burdens of implementation and the entities on whom those burdens will most likely fall.

(ii) identify key U.S. and international stakeholders.

(iii) identify any barriers to implementing the Domain-based Message Authentication, Reporting, and Conformance standard at scale across all U.S.-based email providers.

(iv) propose a strategy to implement the Domain-based Message Authentication, Reporting, and Conformance standard at scale across all U.S.-based email providers, accounting for barriers to implementation and balancing benefits and burdens, where feasible.

(v) provide an initial estimate of the total cost to government and implementing entities in the private sector of implementing the Domain-based Message Authentication, Reporting, and Conformance standard at scale across all U.S.-based email providers and propose recommendations for defraying these costs, if applicable.

(B) CONSULTATION.—In developing the strategy pursuant to paragraph (2) the Department of Homeland Security shall consult with the information technology sector.

(b) DEFINITIONS.—In this Act:

(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) DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING, AND CONFORMANCE (DMARC).—The term "domain-based message authentication, reporting, and conformance (DMARC)" means an email authentication, policy, and reporting protocol that verifies the authenticity of the sender of an email and blocks and reports fraudulent accounts.

(4) INFORMATION AND COMMUNICATIONS TECHNOLOGY INFRASTRUCTURE PROVIDERS.—The term "information and communications technology infrastructure providers" means all systems that enable connectivity and operability of internet service, backbone, cloud, web hosting, content delivery, Domain Name System, and software-defined networks and other systems and services.

## 4.5.3 Strengthen the U.S. Government's Ability to Take Down Botnets

This proposal seeks to implement the Commission's recommendation for Congress to enact section 4 of the "International Cybercrime Prevention Act." This legislation provides courts with broader authority to address illegal botnets. This proposal does not recommend any changes to section 4's language, and does not seek to enact any other sections of the "International Cybercrime Prevention Act."

---

**SEC. 1. STRENGTHEN BOTNET TAKEDOWN.**

(a) Section 1345 of title 18, United States Code, is amended—

(1) in the heading, by inserting "and abuse" after "fraud";

(2) in subsection (a)—

(A) in paragraph (1)—

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

(ii) in subparagraph (C), by inserting "or" after the semicolon; and

(iii) by inserting after subparagraph (C) the following:

"(D) violating section 1030(a)(5) of this title where such conduct has caused or would cause damage (as defined in section 1030) without authorization to 100 or more protected computers (as defined in section 1030) during any 1-year period, including by—

"(i) impairing the availability or integrity of the protected computers without authorization; or

"(ii) installing or maintaining control over malicious software on the protected computers that, without authorization, has caused or would cause damage to the protected computers;"; and

(B) in paragraph (2), by inserting ", a violation described in subsection (a)(1)(D)," before "or a Federal health care offense"; and

(3) by adding at the end the following:

"(c) In issuing a restraining order, prohibition, or other action described in subsection (b), if issued in circumstances described in subsection (a)(1)(D), the court may, upon application of the Attorney General—

"(1) specify that no cause of action shall lie in any court against a person for complying with the restraining order, prohibition, or other action; and

"(2) direct the United States to reimburse reasonable costs which have been incurred as a direct result of complying with the restraining order, prohibition, or other action.".

## 4.6 Develop a National Strategy for the ICT Industrial Base

This proposal directs the U.S. government to assess the United States' information and communications technology (ICT) supply chain and develop and implement an ICT industrial base strategy to reduce dependency and ensure greater security and availability of these critical technologies.

---

**A BILL**

To direct the President to create a national industrial base strategy to ensure the integrity, security, and availability of critical information and communications technology materials, resources, and components, and for other purposes.

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

**SEC. 1. NATIONAL INFORMATION AND COMMUNICATIONS TECHNOLOGY INDUSTRIAL BASE STRATEGY.**

(a) IN GENERAL.—Not later than six months after enactment of this Act, and once every four years thereafter, the President of the United States shall coordinate with the Secretary of Defense, the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of State, and consult with the Director of National Intelligence and private sector entities, to develop a comprehensive national strategy for the information and communications technology (hereinafter in this section referred to as "ICT") industrial base for the following four-year period, or a longer period, if appropriate.

(b) REQUIREMENT.—Each strategy required by subsection (a) shall—

(1) delineate a national ICT industrial base strategy consistent with—

(A) the most recent national security strategy report submitted pursuant to section 108 of the National Security Act of 1947;

(B) the strategic plans of other relevant departments and agencies of the United States; and

(C) other relevant national-level strategic plans;

(2) assess the ICT industrial base, to include identifying—

(A) critical technologies, trusted components, products and materials that comprise or support the ICT industrial base;

(B) industrial capacity of the United States, as well as its allied and partner nations necessary for the manufacture and development of ICT deemed critical to the United States national and economic security; and

(C) areas of supply risk to ICT critical technologies, trusted components, products and materials that comprise or support the ICT industrial base;

(3) identify national ICT strategic priorities and estimate Federal monetary and human resources necessary to fulfill such priorities and areas where strategic financial investment in ICT research and development is necessary for national and economic security; and

(4) assess the Federal government's structure, resourcing, and authorities for evaluating ICT components, products and materials and promoting availability and integrity of trusted technologies.

(c) SUBMISSION OF STRATEGY.—

(1) IN GENERAL.—The President of the United States shall submit the strategy required by this section to the Committees on Homeland Security and Governmental Affairs; Commerce, Science, and Transportation; Armed Services; and Foreign Relations of the Senate; and the Committees on Foreign Affairs; Homeland Security; Energy and Commerce; and Armed Service of the House of Representatives not later than 90 days after the date of the completion of such strategy.

(2) FORM.—The strategy required pursuant to subsection (a) shall be submitted in unclassified form, but may include a classified annex.

(d) DEFINITIONS.—In this section:

(1) INFORMATION AND COMMUNICATIONS TECHNOLOGY.—The term "information and communications technology" means information technology and other equipment, systems, technologies, or processes, for which the principal function is the creation, manipulation, storage, display, receipt, protection or transmission of electronic data and information, as well as any associated content.

(2) INFORMATION AND COMMUNICATIONS TECHNOLOGY INDUSTRIAL BASE STRATEGY.—The term "information and communications technology industrial base strategy" means a set of plans devised to identify critical dependencies on information and communications technologies, components,

or materials and direct Federal resources and investments to bolster trusted information and communications technology industrial capacity and research and development.

## 4.7 Pass a National Data Security and Privacy Protection Law

This proposal seeks to improve the security and privacy of an individual's data by establishing a common framework and minimum standards across the United States for the collection, retention, use, and transfer of an individual's data by covered entities.

---

**A BILL**

To establish a common framework and minimum standards across the United States for the collection, retention, use, and transfer of an individual's data, and for other purposes.

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

**SEC. 1. SHORT TITLE; TABLE OF CONTENTS.**

(a) SHORT TITLE.—This Act may be cited as the "Personal Data Security and Privacy Protection Act of 2020".

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

## SEC. 2. DEFINITIONS.

In this Act:

(1) AFFIRMATIVE EXPRESS CONSENT.—

(A) IN GENERAL.—The term "affirmative express consent" means an affirmative act by an individual that clearly communicates the individual's authorization for a specific processing purpose, in response to a specific request that meets the requirements of subparagraph (B).

(B) REQUEST REQUIREMENTS.—To satisfy the requirements of this subparagraph with respect to a request from a covered entity, the request shall—

(i) be provided to the individual in a standalone disclosure;

(ii) include a description of each processing purpose for which the individual's consent is sought;

(iii) clearly identify and distinguish between a processing purpose that is necessary to fulfill a request made by the individual and a processing purpose that is for another purpose;

(iv) include a prominent heading that would enable a reasonable individual to easily identify and understand the processing purpose for which consent is sought; and

(v) clearly explain the individual's applicable rights related to consent.

(C) EXPRESS CONSENT REQUIRED.—A covered entity shall not infer that an individual has provided affirmative express consent from the inaction of the individual or the individual's continued use of a service or product provided by the covered entity.

(2) COLLECT; COLLECTION.—The terms "collect" and "collection" mean intentionally or unintentionally buying, renting, gathering, obtaining, receiving, accessing, or otherwise acquiring any individual data by any means, including passively or actively observing the individual's behavior.

(3) COMMISSION.—The term "Commission" means the Federal Trade Commission.

(4) COMMON BRANDING.—The term "common branding" means a shared name, servicemark, or trademark that is shared by two or more entities.

(5) CONTROL.—The term "control" means, with respect to an entity—

(A) ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of the entity;

(B) control in any manner over the election of a majority of the directors of the entity (or of individuals exercising similar functions); or

(C) the power to exercise a controlling influence over the management of the entity.

(6) COVERED ENTITY.—

(A) IN GENERAL.—The term "covered entity" means any entity or person that—

(i) operates in or affects interstate or foreign commerce; and

(ii) processes or transfers individual data.

(B) INCLUSION OF COMMONLY CONTROLLED AND COMMONLY BRANDED ENTITIES.—Such term includes any entity or person that controls, is controlled by, is under common control with, or shares common branding with a covered entity.

(C) EXCLUSION OF SMALL BUSINESS.—Such a term does not include a small business.

(D) COMMON CONTROL; COMMON BRANDING.—For purposes of subparagraph (B), the annual average gross revenue, data processing volume, and percentage of annual revenue of an entity shall include the revenue and processing activities of any person that controls, is controlled by, is under common control with, or shares common branding with such entity.

(7) SMALL BUSINESS.—The term "small business" means an entity that can establish that, with respect to the three preceding calendar years (or for the period during which the entity has been in existence if, as of such date, such period is less than three years), the entity did not—

(A) maintain annual average gross revenue in excess of $25,000,000;

(B) annually process the individual data of 100,000 or more individuals, households, or devices used by individuals or households; and

(C) derive 50 percent or more of its annual revenue from transferring individual's individual data.

(8) INDIVIDUAL DATA.—

(A) IN GENERAL.—The term "individual data" means information that directly or indirectly identifies or is linked or reasonably linkable to an individual, or to a household, or a device that is linked or reasonably linkable to an individual or household.

(B) LINKED OR REASONABLY LINKABLE.—For purposes of subparagraph (A), information held by a covered entity is linked or reasonably linkable to an individual or household if, as a practical matter, it can be used on its own or in combination with other information held by, or readily accessible to, the covered entity to identify the individual or household, or a device associated with that individual or household.

(C) EXCLUSIONS.—Such term does not include—

(i) aggregated data;

(ii) de-identified data;

(iii) employee data; and

(iv) publicly available information.

(D) AGGREGATED DATA.—For purposes of subparagraph (C), the term "aggregated data" means information that relates to a group or category of individuals or devices that does not identify and is not linked or reasonably linkable to any individual or household.

(E) DE-IDENTIFIED DATA.—For purposes of subparagraph (C), the term "de-identified data" means information that cannot reasonably be used to identify, or otherwise be linked to, an individual, a household, or a device used by an individual or household, provided that the entity—

(i) takes reasonable measures to ensure that the information cannot be reidentified, or associated with, an individual, a household, or a device used by an individual or household;

(ii) publicly commits in a conspicuous manner—

(I) to process and transfer the information in a de-identified form;

(II) not to attempt to reidentify or associate the information with any individual, household, or device used by an individual or household; and

(III) to adopt technical and organizational measures to ensure that the information is not linked to any individual, household, or device used by an individual or household; and

(iii) is not disclosed by the covered entity to any other person or entity unless the disclosure is subject to a contractually or other legally binding requirement to comply with all of the provisions of this paragraph.

(F) EMPLOYEE DATA.—For purposes of subparagraph (C), the term "employee data" means—

(i) information relating to an individual collected by a covered entity or the covered entity's service provider about an individual in the course of the individual's employment or application for

employment (including on a contract or temporary basis) provided that such information is collected, processed, or transferred by the covered entity or the covered entity's service provider solely for purposes related to the individual's employment or application for employment; and

(ii) business contact information of an individual, including the individual's name, position name or title, business telephone number, business address, business email address, qualifications, and other similar information, that is provided to a covered entity by an individual who is acting in a professional capacity, provided that such information is collected, processed, or transferred solely for purposes related to such individual's professional activities.

(G) PUBLICLY AVAILABLE INFORMATION.—For the purposes of subparagraph (C), the term "publicly available information"—

(i) means any information that—

(I) has been lawfully made available to the general public from Federal, State, or local government records, not directly disclosed by the individual;

(II) is widely available to the general public, including information from—

(aa) a telephone book or online directory;

(bb) a television, internet, or radio program; or

(cc) the news media or a website that is available to the general public on an unrestricted basis (for purposes of this subclause a website is not restricted solely because there is a fee or log-in requirement associated with accessing the website); or

(III) a disclosure by the individual to the general public that is made voluntarily; and

(ii) does not include an obscene visual depiction (as defined for purposes of section 1460 of title 18, United States Code).

(9) DATA BROKER.—The term "data broker" means a covered entity that knowingly collects or processes on behalf of, or transfers to, third parties the individual data of an individual with whom the entity does not have a direct relationship.

(10) DERIVED DATA.—The term "derived data" means information that is created through the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source or information or data about an individual, household, or device used by an individual or household.

(11) DELETE.—The term "delete" means to remove or destroy information such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.

(12) INDIVIDUAL.—The term "individual" means a natural person residing or located in the United States, however identified, including by any unique identifier.

(13) LARGE DATA HOLDER.—The term "large data holder" means a covered entity that in the most recent calendar year processed or transferred the—

(A) individual data of more than 5,000,000 individuals, devices used by individuals or households, or households; or

(B) sensitive individual data of more than 100,000 individuals, devices used by individuals or households, or households (excluding any instance where the covered entity processes the log-in information of an individual, device, or household to allow the individual, device, or household to log-in to an account administered by the covered entity).

(14) MATERIAL.—The term "material" means, with respect to an act, practice, or representation of a covered entity (including a representation made by the covered entity in a privacy policy or similar disclosure to an individual or the public), that such act, practice, or representation is likely to affect an individual's decision or conduct regarding a product or service.

(15) PROCESS.—The term "process" means any operation or set of operations performed on the data in question including collection, analysis, organization, structuring, retaining, using, or otherwise handling the data in question.

(16) PROCESSING PURPOSE.—The term "processing purpose" means an adequately specific and granular reason for which a covered entity processes the data in question that is specific enough for a reasonable individual to understand the processing activity.

(17) SENSITIVE INDIVIDUAL DATA.—The term "sensitive individual data" means any of the following forms of individual data:

(A) A unique, government-issued identifier, such as a Social Security number, passport number, or driver's license number.

(B) Any information that describes or reveals the past, present, or future physical health, mental health, disability, diagnosis, or treatment of an individual.

(C) A financial account number, debit card number, credit card number, or any required security or access code, password, or credentials allowing access to any such account.

(D) Precise geolocation information capable of determining with reasonable specificity the past or present actual physical location of an individual, device, or household at a specific point in time.

(E) The content or metadata of an individual's private communications or the identity of the parties to such communication, unless the covered entity is an intended recipient of the communication.

(F) Account log-in credentials such as a username or email address, in combination with a password or security question and answer that would permit access to an online account.

(G) Information revealing an individual's race, ethnicity, national origin, or religion.

(H) Information revealing the sexual orientation or sexual behavior of an individual.

(I) Information about online activities that relate to a category of individual data described in another subparagraph of this paragraph.

(J) Information such as calendar information, address book information, phone or text logs, photos, or videos maintained on an individual's device.

(K) Information revealing union membership or lack of union membership.

(L) A photograph, film, video recording, or other similar medium that shows the naked or undergarment-clad private area of an individual.

(M) Any individual data processed by a covered entity for the purpose of identifying information described in another subparagraph of this paragraph.

(N) Any other category of individual data designated by the Commission pursuant to a rulemaking under section 553 of title 5, United States Code, if the Commission determines that the processing or transfer of individual data in such category in a manner that is inconsistent with the

reasonable expectations of an individual would be likely to be offensive to a reasonable individual.

(18) SERVICE PROVIDER.—

(A) IN GENERAL.—The term "service provider" means a covered entity that processes or transfers individual data for the purpose of performing one or more services or functions on behalf of, and at the direction of, another covered entity that is not related to the covered entity providing the service of function by common ownership or corporate control and does not share common branding with the covered entity providing the service or function, but only to the extent that such processing or transferal—

(i) relates to the performance of such service or function; or

(ii) is necessary to comply with a legal obligation or to establish, exercise, or defend legal claims.

(B) EXCLUSIONS.—Such term does not include a covered entity that processes or transfers the individual data outside of the direct relationship between the service provider and the covered entity.

(19) SERVICE PROVIDER DATA.—The term "service provider data" means individual data that is collected by the service provider on behalf of a covered entity or transferred to the service provider by a covered entity for the purpose of allowing the service provider to perform a service or function on behalf of, and at the direction of, such covered entity.

(20) THIRD PARTY.—The term "third party" means a covered entity that—

(A) is not a service provider with respect to such data; and

(B) received such individual data from another covered entity that—

(i) is not related to the covered entity by common ownership or corporate control; and

(ii) does not share common branding with the covered entity.

(21) THIRD PARTY DATA.—The term "third party data" means individual data that is transferred to a third party by a covered entity.

(22) TRANSFER.—The term "transfer" means to intentionally disclose, release, share, disseminate, make available, sell, license, or otherwise communicate individual

data by any means for consideration or gain of any kind or for a commercial purpose.

(23) UNIQUE IDENTIFIER.—The term "unique identifier" means an identifier that is reasonably linkable to an individual, household, or device used by an individual or household, including a device identifier, an Internet Protocol address, cookies, beacons, pixel tags, mobile ad identifiers, or similar technology, customer number, unique pseudonym, or user alias, telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular individual, household, or device.

## SEC. 3. EFFECTIVE DATE.

Except as otherwise provided in this Act, this Act shall take effect 12 months after the date of the enactment of this Act.

# TITLE I—DATA SECURITY AND RETENTION

## SEC. 101. DATA SECURITY.

(a) IN GENERAL.—A covered entity shall establish, implement, and maintain reasonable administrative, technical, and physical data security policies and practices to protect the confidentiality, integrity, availability, security, and accessibility of individual data.

(b) DATA SECURITY REQUIREMENTS.— The data security policies and practices required under subsection (a) shall be, at a minimum—

(1) appropriate to the size and complexity of the covered entity, the nature and scope of the covered entity's collection or processing of individual data, and the nature and volume of the individual data at issue; and

(2) designed to—

(A) identify and assess reasonably foreseeable human or technical risks or vulnerabilities to individual data, including unauthorized access, access rights, and use of service providers;

(B) take preventative and corrective action to address anticipated and known risks or vulnerabilities to individual data, which may include implementing administrative, technical, or physical safeguards or changes to data security policies or practices; and

(C) receive and respond to unsolicited reports of vulnerabilities by entities and individuals.

(c) TRAINING.—The data security policies required under subsection (a) shall provide for training all employees with access to individual data on how to safeguard individual data and protect individual privacy and updating that training as necessary; and training for all employees designing or procuring such systems which processes, maintain, or transfer individual data.

(d) RULEMAKING.—

(1) IN GENERAL.—The Commission may, pursuant to a proceeding in accordance with section 553 of title 5, United State Code, issue regulations to identify processes for receiving and assessing information regarding vulnerabilities to individual data that are reported to the covered entity.

(2) CONSULTATION WITH NIST.—In promulgating regulations under this subsection, the Commission shall consult with, and take into consideration guidance from, the National Institute of Standards and Technology.

(e) GUIDANCE.—Not later than one year after the date of enactment of this Act, the Commission shall issue guidance to covered entities on how to—

(1) identify and assess vulnerabilities to individual data, including—

(A) the potential for unauthorized access to individual data;

(B) human or technical risks or vulnerabilities to individual data;

(C) the management of access rights; and

(D) the use of service providers to process individual data;

(2) take preventative and corrective action to address risks and vulnerabilities to individual data; and

(3) provide effective data security and privacy training as described in subsection (c), in conjunction with the National Institute of Standards and Technology.

(f) APPLICABILITY OF OTHER INFORMATION SECURITY LAWS.—A covered entity that is required to comply with title V of the Gramm-Leach-Bliley Act (15 U.S.C 6801 et seq.), the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq.), part C of title XI of the Social Security Act (42 U.S.C. 6801 et seq.), or the regulations promulgated pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d-2 note), and is in compliance with the information security requirements of such regulations, part, title, or Act (as applicable), shall be deemed to be in compliance with the

requirements of this section with respect to data subject to requirements of such regulations, part, title, or Act.

**SEC. 102. DATA RETENTION AND DISPOSAL.**

(a) IN GENERAL.—A covered entity shall delete individual data after it is no longer necessary for the purpose for which it was collected. Such process shall include destroying, permanently erasing, or otherwise modifying the individual data to make such data permanently unreadable or indecipherable and unrecoverable and data hygiene practices to ensure ongoing compliance with this section.

(b) FIVE YEARS.—A covered entity shall delete individual data five years after it is collected.

(c) EXCEPTIONS.—A covered entity may retain individual data if—

(1) an individual has provided affirmative express consent to such retention;

(2) such retention is necessary to comply with a law; or

(3) under such exceptions, waivers, or exclusions as the Commission may provide consistent with the purpose of this Act.

**SEC. 103. MINIMIZATION OF DATA COLLECTION, PROCESSING, AND TRANSFER.**

(a) IN GENERAL.—A covered entity shall not collect, process, or transfer individual data beyond what is reasonably necessary, proportionate, and limited—

(1) to carry out the specific processing purposes and transfers described in the privacy policy made available by the covered entity under section 201;

(2) to carry out a specific processing purpose or transfer for which the covered entity has obtained affirmative express consent;

(3) for a purpose specifically permitted under section 205; or

(4) to comply with required disclosures of data to Federal, State, local, tribal, or territorial regulatory entities.

(b) BEST PRACTICES.—Not later than one year after the date of enactment of this Act, the Commission shall issue guidelines recommending best practices for covered entities to minimize the collection, processing, and transfer of individual data in accordance with this section.

## TITLE II—DATA USE

### SEC. 201. TRANSPARENCY.

(a) IN GENERAL.—A covered entity shall, with respect to each service or product provided by the covered entity, publish a privacy policy that is—

(1) disclosed, in a clear and conspicuous manner, to an individual prior to or at the point of the collection of the individual data from the individual; and

(2) made publicly and persistently available, in a conspicuous and readily accessible manner, to the public.

(b) CONTENT.—The privacy policy required under subsection (a) shall include, at a minimum—

(1) the identity and contact information of the covered entity, including the contact information for the covered entity for data security and privacy inquiries;

(2) each category of data the covered entity collects and the processing purposes for which such data is collected;

(3) whether the covered entity transfers individual data and, if so—

(A) each category of service provider and third party to which the covered entity transfers individual data and the purposes for which such data is transferred to such categories; and

(B) the identity of each third party to which the covered entity transfers individual data and the purposes for which such data is transferred to such third party, except for transfers to governmental entities, transfers pursuant to a court order or law that prohibits the covered entity from disclosing such transfer;

(4) a detailed description of the covered entity's data retention practices for individual data, the purposes for such retention, and how long individual data processed by the covered entity will be retained;

(5) a description of the covered entity's data minimization policies;

(6) information about how individuals can exercise the rights described in this Act;

(7) a general description of the covered entity's data security practices; and

(8) the effective date of the covered entity's privacy policy.

(c) LANGUAGES.—A covered entity shall make the privacy policy required under this section available in all of the languages in which the covered entity provides a product or service or carries out any other activities to which the privacy policy relates.

(d) MATERIAL CHANGES.—A covered entity shall not make a material change to its privacy policy or practices with respect to previously collected individual data that would weaken the privacy protections applicable to such data without first obtaining prior affirmative express consent in easily understood language and a clear and readable format from the individuals affected. The covered entity shall provide direct notification, where practicable, regarding material changes to affected individuals, taking into account available technology, readability, the consumer's ability to understand the notification, and the nature of the relationship.

(e) ALGORITHM TRANSPARENCY STUDY AND REPORTS.—

(1) STUDY.—The Commission shall conduct a study, conducted using the Commission's authority under section 6(b) of the Federal Trade Commission Act (15 U.S.C. 46(b)), examining the use of algorithms to process individual data in a manner that may violate Federal anti-discrimination laws.

(2) REPORT.—Not later than three years after the date of enactment of this Act, the Commission shall publish a report containing the results of the study required under paragraph (A).

(3) GUIDANCE.—The Commission shall use the results of the study described in subparagraph (A) to develop guidance to assist covered entities in avoiding discriminatory use of algorithms.

(4) UPDATED REPORT.—Not later than five years after the publication of the report required under this subsection, the Commission shall publish an updated report.

**SEC. 202. ACCESS TO, CORRECTION, DELETION, AND PORTABILITY OF INDIVIDUAL DATA.**

(a) IN GENERAL.—Subject to subsections (b) and (c), a covered entity shall respond to an individual, in a human-readable format that a reasonable individual can understand, immediately or as quickly as practicable and in no case later than 45 days after receiving a verified request from the individual, as follows:

(1) REQUESTS FOR ACCESS.—Upon request for access to the individual data for an individual, the covered entity shall provide—

(A) a description of the individual data of the individual, or an accurate representation of the individual data of the individual, that is processed or transferred by the covered entity;

(B) a list of names of service providers or third parties to whom individual data has been transferred by the covered entity; and

(C) a description of each purpose for which the covered entity transferred the individual data to a service provider or third party.

(2) REQUESTS FOR CORRECTION.—Upon request to correct errors in the individual's individual data, the covered entity shall—

(A) correct, or allow the individual to correct, inaccurate or incomplete information in the individual data of the individual that is processed by the covered entity; and

(B) inform any service provider or third party to which the covered entity transferred such individual data of the corrected information.

(3) REQUEST FOR DELETION.—Upon request to delete the individual's individual data, the covered entity shall—

(A) delete, allow the individual to delete, or de-identify any information in the individual data of the individual that is processed by the covered entity; and

(B) inform any service provider or third party to which the covered entity transferred such individual data of the individual's request.

(4) REQUEST FOR EXPORT.—Upon an individual's request to export the individual's individual data, the covered entity shall, to the extent technically feasible, export the individual's individual data, except for derived data, without licensing restrictions—

(A) in a human-readable format that allows the individual to understand such individual data of the individual; and

(B) in a portable, structured, standards-based, interoperable, and machine-readable format that includes all individual data or other information that the covered entity collected to the extent feasible.

(b) FREQUENCY AND COST OF ACCESS.—A covered entity shall—

(1) provide an individual with the opportunity to exercise the rights described in each paragraph of subsection (a) not less than twice during any 12-month period; and

(2) with respect to the first eight times that an individual exercises the rights described in subsection (a) in any 12-month period, allow the individual to exercise such rights free of charge.

(c) VERIFICATION.—A covered entity shall not comply with a request to exercise the rights described in subsection (a) if the covered entity cannot verify that the individual making the request is the individual to whom the individual data that is the subject of the request relates or an individual authorized to make such a request on the individual's behalf.

(d) EXCEPTIONS.—A covered entity may decline to comply with a request that would—

(1) require the entity to retain any individual data for the sole purpose of fulfilling the request;

(2) prevent the covered entity from carrying out internal audits, performing accounting functions, processing refunds, or fulfilling warranty claims, provided that the individual data that is subject to the request is not processed or transferred for any purpose other than such specific activities;

(3) impair the publication of newsworthy information of legitimate public concern to the public by a covered entity, or the processing or transfer of information by a covered entity for such a purpose;

(4) impair the privacy of another individual or the rights of another to exercise free speech;

(5) be impossible or demonstrably impracticable to comply with; or

(6) require the covered entity to re-identify individual data that has been deidentified.

(e) REGULATIONS.—Not later than one year after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, establishing and clarifying requirements for covered entities with respect to the verification of requests to exercise rights described in this section.

## SEC. 203. INDIVIDUAL CONSENT.

(a) SENSITIVE INDIVIDUAL DATA.—A covered entity shall not, without the prior, affirmative express consent of the individual to whom the individual data relates, process or transfer sensitive individual data.

(b) INDIVIDUAL DATA.—Except as provided in section 205, a covered entity shall not, if the individual who the data relates objects—

(1) process the individual's individual data after the objection; or

(2) transfer of the individual's individual data to a third party after the objection.

(c) WITHDRAWAL OF CONSENT.—A covered entity shall provide an individual a clear and conspicuous means, in language which a reasonable individual can understand, to withdraw both, or either, affirmative express consent and objections described in subsections (a) and (b).

(d) RULEMAKING.—The Commission may promulgate regulations under section 553 of title 5, United States Code, to provide guidance on one or more acceptable processes for covered entities to follow to allow individuals to provide and withdraw both affirmative express consent and objections as described in subsections (a) and (b).

(e) MINORS.—

(1) PARENTAL CONSENT.—A parent or legal guardian may provide affirmative express consent on behalf of an individual who is less than 18 years of age.

(2) PRIOR CONSENT TO TRANSFER OF CHILDREN'S DATA.—A covered entity shall not transfer the individual data of an individual to a third-party without affirmative express consent from the individual's parent or guardian if the covered entity has actual knowledge that the individual is less than 13 years of age.

## SEC. 204. SERVICE PROVIDERS AND THIRD PARTIES.

(a) SERVICE PROVIDERS.—A service provider—

(1) shall not process service provider data for any processing purpose that is not performed on behalf of, and at the direction of, the covered entity that transferred the data to the service provider, except that a service provider may process data to comply with a legal obligation or the establishment, exercise, or defense of legal claims;

(2) shall not transfer service provider data to a third party without the affirmative express consent, obtained by, or on behalf of, the covered entity, of the individual to whom the service provider data relates;

(3) shall delete or de-identify service provider data—

(A) as soon as practicable after the service provider has completed providing the service or function for which the data was transferred to the service provider; or

(B) as soon as practicable after the end of the period during which the service provider is to provide services with respect to such data, as agreed to by the service provider and the covered entity that transferred the data;

(4) is exempt from the requirements of section 202 with respect to service provider data, but shall, to the extent practicable—

(A) assist the covered entity from which it received the service provider data in fulfilling requests made by individuals under such sections; and

(B) shall delete, de-identify, or correct (as applicable), any service provider data that is subject to a verified request from an individual described in section 202(a)(ii) or (iii); and

(5) is exempt from the requirements of section 103 with respect to service provider data, but shall have the same responsibilities and obligations as a covered entity with respect to such data under all other provisions of this Act.

(b) THIRD PARTIES.—A third party—

(1) shall not process third party data for a processing purpose inconsistent with the reasonable expectation of the individual to whom such data relates;

(2) for purposes of paragraph (1), may reasonably rely on representations made by the covered entity that transferred third party data regarding the reasonable expectations of individuals to whom such data relates, provided that the third party conducts reasonable due diligence on the representations of the covered entity and finds those representations to be credible; and

(3) upon receipt of any third party data, is exempt from the requirements of section 103 and section 204(a) with respect to such data, but shall have the same responsibilities and obligations as a covered entity with respect to such data under all other provisions of this Act.

(c) ADDITIONAL OBLIGATIONS ON COVERED ENTITIES.—

(1) IN GENERAL.—A covered entity shall—

(A) exercise reasonable due diligence in selecting a service provider and conduct reasonable oversight of its service providers to ensure compliance with the applicable requirements of this section; and

(B) exercise reasonable due diligence before deciding to transfer individual data to a third party, and conduct oversight of third parties to which it transfers data to ensure compliance with the applicable requirements of this subsection.

(2) GUIDANCE.—Not later than 18 months after the effective date of this Act, the Commission shall publish guidance regarding compliance with this subsection. Such guidance shall, to the extent practicable, minimize unreasonable burdens on small and medium-sized covered entities.

**SEC. 205. SCOPE OF COVERAGE.**

(a) IN GENERAL.—Notwithstanding any provision of this Act other than sections 201, 202, and 301, a covered entity may collect, process, or transfer individual data for any of the following purposes, provided that the collection, processing, or transfer is reasonably necessary, proportionate, and limited to such purpose:

(1) To complete a transaction of fulfilling an order or service specifically requested by an individual, including associated routine administrative activities such as billing, shipping, and account.

(2) To perform system maintenance, debug systems, or repair errors to ensure the functionality of a product or service provided by the covered entity.

(3) To detect or respond to a security incident, provide a secure environment, or maintain the safety of a product or service.

(4) To protect against malicious, deceptive, fraudulent, or illegal activity.

(5) To comply with a legal obligation or the establishment, exercise, or defense of legal claims.

(6) To prevent an individual from suffering harm where the covered entity believes in good faith that the individual is in danger of suffering death or serious injury.

(7) To effectuate a product recall pursuant to Federal or State law.

(8) To conduct scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board or a similar oversight entity that meets standards promulgated by the Commission pursuant to section 553 of title 5, United States Code.

## TITLE III—ACCOUNTABILITY

### SEC. 301. PROHIBITION ON WAIVER OF RIGHTS.

(a) PROHIBITION ON DENIAL.—Unless necessary to provide the good or service, a covered entity shall not—

(1) condition the provision of a good or service to an individual on the individual's agreement to waive rights guaranteed by this Act; or

(2) deny goods or services to an individual because the individual exercised any of the rights established under this Act unless the delivery of the good or service is predicated on the release of such information.

(b) NO WAIVER OF INDIVIDUAL CONTROLS.—The rights and obligations created under section 203 may not be waived in an agreement between a covered entity and an individual.

### SEC. 302. DATA SECURITY OFFICER AND PRIVACY OFFICER.

(a) IN GENERAL.—A covered entity shall designate—

(1) one or more qualified employees as data security officers; and

(2) one or more qualified employees (in addition to any employees designated under paragraph (1)) as privacy officers.

(b) RESPONSIBILITIES.—An employee who is designated by a covered entity as a data security officer or privacy officer shall be responsible for, at a minimum—

(1) coordinating the covered entity's policies and practices regarding the processing of individual data; and

(2) facilitating the covered entity's compliance with this Act.

### SEC. 303. LARGE DATA HOLDERS.

(a) IN GENERAL.—Beginning 18 months after the effective date of this Act, the chief executive officer of a covered entity that is a large data holder (of, if the entity does

not have a chief executive officer, the highest ranking officer of the entity) and each data security officer and privacy officer of such entity shall annually certify to the Commission, in a manner specified by the Commission, that the entity maintains—

(1) adequate internal controls to comply with this Act; and

(2) reporting structures to ensure that such certifying officers are involved in, and are responsible for, decisions that impact the entity's compliance with this Act.

(b) REQUIREMENTS.—A certification submitted under subsection (a) shall be based on a review of the effectiveness of a covered entity's internal controls and reporting structures that is conducted by the certifying officers no more than 90 days before the submission of the certification.

**SEC. 304. DATA BROKERS.**

(a) IN GENERAL.—Not later than January 31 of each calendar year that follows a calendar year during which a covered entity acted as a data broker, such covered entity shall register with the Commission pursuant to the requirements of this section.

(b) REGISTRATION REQUIREMENTS.—In registering with the Commission as required under subsection (a), a data broker shall do the following:

(1) Pay to the Commission a registration fee of $100.

(2) Provide the Commission with the following information:

(A) The name and primary physical, email, and internet addresses of the data broker.

(B) Any additional information or explanation the data broker chooses to provide concerning its data collection and processing practices.

(3) PENALTIES.—A data broker that fails to register as required under subsection (a) of this section shall be liable for—

(A) a civil penalty of $50 for each day it fails to register, not to exceed a total of $10,000 for each year; and

(B) an amount equal to the fees due under this section for each year that it failed to register as required under subsection (a).

(4) PUBLICATION OF REGISTRATION INFORMATION.—The Commission shall publish on the internet website of the Commission the registration information provided by data brokers under this section.

## SEC. 305. ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.

(a) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of this Act or a regulation promulgated under this Act shall be treated as a violation of a rule defining an unfair or deceptive practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57(a)(1)(B)).

(b) POWERS OF COMMISSION.—

(1) IN GENERAL.—Except as provided in subsections (d) and (e), the Commission shall enforce this Act and the regulations promulgated under this Act 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 Act.

(2) PRIVILEGES AND IMMUNITIES.—Any person who violates this Act or a regulation promulgated under this Act 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.).

(3) AUTHORITY PRESERVED.—Nothing in this Act shall be construed to limit the authority of the Commission under any other provision of law, except as it applies to the data security and data privacy requirements and regulations promulgated under this Act.

(c) COMMISSION RESOURCES.—

(1) APPOINTMENT OF ATTORNEYS, TECHNOLOGISTS, AND SUPPORT PERSONNEL.—Notwithstanding any other provision of law, the Chair of the Commission shall appoint no fewer than 400 additional individuals to serve as personnel to enforce this Act and other laws relating to privacy and data security that the Commission is authorized to enforce.

(2) ASSESSMENT OF COMMISSION RESOURCES.—Not later than one year after the date of enactment of this Act, the Commission shall submit to Congress a report that includes—

(A) an assessment of the resources, including personnel, available to the Commission to carry out this Act; and

(B) a description of any resources, including personnel—

(i) that are not available to the Commission; and

(ii) that the Commission requires to effectively carry out this Act.

(d) COMMON CARRIERS AND NONPROFIT ORGANIZATIONS.—Notwithstanding section 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 Commission, the Commission shall also enforce this Act and the regulations promulgated under this Act, in the same manner as provided in subsections (a) and (b) of this section, with respect to—

(1) common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.) and all Acts amendatory thereof and supplementary thereto; and

(2) organizations not organized to carry on business for their own profit or that of their members.

(e) DATA SECURITY AND PRIVACY FUND.—

(1) ESTABLISHMENT OF RELIEF FUND.—There is established in the Treasury of the United States a separate fund to be known as the "Data Security and Privacy Relief Fund" (referred to in this paragraph as the "Relief Fund"),

(2) DEPOSITS.—

(A) DEPOSITS FROM THE COMMISSION.—The Commission shall deposit into the Relief Fund the amount of any civil penalty obtained against any covered entity in any judicial or administrative action the Commission commences to enforce this Act or a regulation promulgated under this Act.

(B) DEPOSITS FROM THE ATTORNEY GENERAL.—The Attorney General of the United States shall deposit into the Relief Fund the amount of any civil penalty obtained against any covered entity in any judicial or administrative action the Attorney General commences on behalf of the Commission to enforce this Act or a regulation promulgated under this Act.

(3) USE OF FUND AMOUNTS.—Notwithstanding section 3302 of title 31, United States Code, amounts in the Relief Fund shall be available to the Commission, without fiscal year limitation, to provide redress, payments or compensation, or other monetary relief to individuals affected by an act or practice for which civil penalties have been imposed under this Act. To the extent that individuals cannot be located or such redress, payments or

compensation, or other monetary relief are otherwise not practicable, the Commission may use such funds for the purpose of consumer or business education relating to data security and privacy or for the purpose of engaging in technological research that the Commission considers necessary to enforce this Act.

(4) AMOUNTS NOT SUBJECT TO APPORTIONMENT.—Notwithstanding any other provision of law, amounts in the Relief Fund shall not be subject to apportionment for purposes of chapter 15 of title 31, United States Code, or under any other authority.

**SEC. 306. INTERNATIONAL COORDINATION AND COOPERATION**.

(a) IN GENERAL.—If necessary, the Commission shall coordinate any enforcement action by the Commission under this Act with any relevant data protection authority established by a foreign country or any similar office of a foreign country in a manner consistent with subsections (j) and (k) of section 6 of the Federal Trade Commission Act (15 U.S.C. 20 46).

(b) INTERNATIONAL INTEROPERABILITY.—The Secretary of Commerce, in consultation with the Commission and the heads of other relevant Federal agencies, shall—

(1) identify laws of foreign countries or regions that relate to the processing of personal data for commercial purposes;

(2) engage with relevant officials of foreign countries or regions that have implemented laws described in paragraph (1) in order to identify requirements under those laws that could disrupt cross-border transfers of personal data;

(3) develop mechanisms and recommendations to prevent disruptions described in paragraph (2); and

(4) not later than one year after the date of enactment of this Act, and once a year each year thereafter for five years, submit to Congress a report on the progress of efforts made under this section.

## TITLE IV—MISCELLANEOUS

**SEC. 401. CONSTITUTIONAL AVOIDANCE.**

The provisions of this Act shall be construed, to the greatest extent practicable, to avoid conflicting with the Constitution of the United States, including the protections established under the First Amendment to the Constitution of the United States.

## SEC. 402. SEVERABILITY.

If any provision of this Act, or an amendment made by this Act, is determined to be unenforceable or invalid, the remaining provisions of this Act and the amendments made by this Act shall not be affected.

## SEC. 403. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to the Commission such sums as may be necessary to carry out this Act.

## 4.7.1 Pass a National Data Breach Notification Law

The proposal establishes a unified national standard for when entities are required to notify authorities and their customers of a data breach (regardless of cause). This standard should 1) preempt existing State, district, and territorial laws, 2) establish definitions and thresholds for covered breaches, 3) require the transmission of appropriate forensic data to law enforcement and cybersecurity authorities, 4) set timelines and standards for victim notification and protection, and 5) deconflict existing Federal regulation for private-sector and non-Federal entities.

---

**A BILL**

To establish a national data breach notification standard, and for other purposes.

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

**SEC. 1. SHORT TITLE; TABLE OF CONTENTS.**

(a) SHORT TITLE.—This Act may be cited as the "Personal Data Notification and Protection Act of 2017".

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

## SEC. 2. NOTIFICATION TO INDIVIDUALS.

(a) IN GENERAL.—Except as provided in section 3, any business entity engaged in or affecting interstate commerce, that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information about more than 10,000 individuals during any 12-month period shall, following the discovery of a security breach of such information, notify, in accordance with sections 4 and 5, any individual whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed or acquired.

(b) OBLIGATIONS OF AND TO OWNER OR LICENSEE.—

(1) NOTIFICATION TO OWNER OR LICENSEE.—Any business entity engaged in or affecting interstate commerce, that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information that the business entity does not own or license shall notify the owner or licensee of the information following the discovery of a security breach involving such information, unless there is no reasonable risk of harm or fraud to such owner or licensee.

(2) NOTIFICATION BY OWNER, LICENSEE, OR OTHER DESIGNATED THIRD PARTY.—Nothing in this Act shall prevent or abrogate an agreement between a business entity required to provide notification under this section and a designated third party, including an owner or licensee of the sensitive personally identifiable information subject to the security breach, to provide the notifications required under subsection (a).

(3) BUSINESS ENTITY RELIEVED FROM GIVING NOTIFICATION.—A business entity required to provide notification under subsection (a) shall not be required to provide such notification if an owner or licensee of the sensitive personally identifiable information subject to the security breach, or other designated third party, provides such notification.

(c) TIMELINESS OF NOTIFICATION.—

(1) IN GENERAL.—All notifications required under this section shall be made without unreasonable delay following the discovery by the business entity of a security breach. A business entity shall, upon the request of the

Commission, provide records or other evidence of the notifications required under this section.

(2) REASONABLE DELAY.—

(A) IN GENERAL.—Except as provided in subsection (d), reasonable delay under this subsection shall not exceed 30 days, unless the business entity seeking additional time requests an extension of time and the Commission determines that additional time is reasonably necessary to determine the scope of the security breach, prevent further disclosures, conduct the risk assessment, restore the reasonable integrity of the data system, or provide notice to the breach notification entity.

(B) EXTENSION.—If the Commission determines that additional time is reasonably necessary as described in subparagraph (A), the Commission may extend the time period for notification for additional periods of up to 30 days each. Any such extension shall be provided in writing by the Commission.

(3) BURDEN OF PRODUCTION.—If a business entity requires additional time under paragraph (2), the business entity shall provide the Commission with records or other evidence of the reasons necessitating delay of notification.

(d) DELAY OF NOTIFICATION FOR LAW ENFORCEMENT OR NATIONAL SECURITY.—

(1) IN GENERAL.—If the Director of the United States Secret Service or the Director of the Federal Bureau of Investigation determines that the notification required under this section would impede a criminal investigation or national security activity, the time period for notification shall be extended 30 days upon written notice from such Director to the business entity that experienced the breach.

(2) EXTENDED DELAY OF NOTIFICATION.—If the time period for notification required under subsection (a) is extended pursuant to paragraph (1), a business entity shall provide the notification within such time period unless the Director of the United States Secret Service or the Director of the Federal Bureau of Investigation provides written notification that further extension of the time period is necessary. The Director of the United States Secret Service or the Director of the Federal Bureau of Investigation may extend the time period for additional periods of up to 30 days each.

(3) IMMUNITY.—No cause of action for which jurisdiction is based under section 1346(b) of title 28, United States Code, shall lie against any Federal law

enforcement agency for acts relating to the extension of the deadline for notification for law enforcement or national security purposes under this section.

(e) DESIGNATION OF BREACH NOTIFICATION ENTITY.—Not later than 60 days after the date of the enactment of this Act, the Secretary of Homeland Security shall designate a Federal government entity to receive notices, reports, and information about information security incidents, threats, and vulnerabilities under this Act.

**SEC. 3. EXEMPTIONS FROM NOTIFICATION TO INDIVIDUALS.**

(a) EXEMPTION FOR NATIONAL SECURITY AND LAW ENFORCEMENT.—

(1) IN GENERAL.—Notwithstanding section 2, if the Director of the United States Secret Service or the Director of the Federal Bureau of Investigation determines that notification of the security breach required by such section could be expected to reveal sensitive sources and methods or similarly impede the ability of a Federal, State, or local law enforcement agency to conduct law enforcement investigations, or if the Director of the Federal Bureau of Investigation determines that notification of the security breach could be expected to cause damage to national security, such notification is not required.

(2) IMMUNITY.—No cause of action for which jurisdiction is based under section 1346(b) of title 28, United States Code, shall lie against any Federal law enforcement agency for acts relating to provision of an exemption from notification for law enforcement or national security purposes under this section.

(b) SAFE HARBOR.—

(1) IN GENERAL.—A business entity is exempt from the notification requirement under section 2, if the following requirements are met:

(A) RISK ASSESSMENT.—A risk assessment, in accordance with paragraph (3), is conducted by or on behalf of the business entity that concludes that there is no reasonable risk that a security breach has resulted in, or will result in, harm to the individuals whose sensitive personally identifiable information was subject to the security breach.

(B) NOTICE TO COMMISSION.—Without unreasonable delay and not later than 30 days after the discovery of a security breach, unless extended by the Commission, the Director of the United States Secret Service, or the Director of the Federal Bureau of Investigation under section 2

(in which case, before the extended deadline), the business entity notifies the Commission, in writing, of—

(i) the results of the risk assessment; and

(ii) the decision by the business entity to invoke the risk assessment exemption described under subparagraph (A).

(C) DETERMINATION BY COMMISSION.—During the period beginning on the date on which the notification described in subparagraph (B) is submitted and ending ten days after such date, the Commission has not issued a determination in writing that a notification should be provided under section 2.

(2) REBUTTABLE PRESUMPTION.—For purposes of paragraph (1)—

(A) the rendering of sensitive personally identifiable information at issue unusable, unreadable, or indecipherable through a security technology generally accepted by experts in the field of information security shall establish a rebuttable presumption that such reasonable risk does not exist; and

(B) any such presumption shall be rebuttable by facts demonstrating that the security technologies or methodologies in a specific case have been, or are reasonably likely to have been, compromised.

(3) RISK ASSESSMENT REQUIREMENTS.—A risk assessment is in accordance with this paragraph if the following requirements are met:

(A) PROPERLY CONDUCTED.—The risk assessment is conducted in a reasonable manner or according to standards generally accepted by experts in the field of information security.

(B) LOGGING DATA REQUIRED.—The risk assessment includes logging data, as applicable and to the extent available, for a period of at least six months before the discovery of a security breach described in section 2(a)—

(i) for each communication or attempted communication with a database or data system containing sensitive personally identifiable information, the data system communication information for the communication or attempted communication, including any Internet addresses, and the date

and time associated with the communication or attempted communication; and

(ii) all log-in information associated with databases or data systems containing sensitive personally identifiable information, including both administrator and user log-in information.

(C) FRAUDULENT OR MISLEADING INFORMATION.—The risk assessment does not contain fraudulent or deliberately misleading information.

(c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

(1) IN GENERAL.—A business entity is exempt from the notification requirement under section 2 if the business entity uses or participates in a security program that—

(A) effectively blocks the use of the sensitive personally identifiable information to initiate unauthorized financial transactions before they are charged to the account of the individual; and

(B) provides notification to affected individuals after a security breach that has resulted in fraud or unauthorized transactions.

(2) LIMITATION.—The exemption in paragraph (1) does not apply if the information subject to the security breach includes the individual's first and last name or any other type of sensitive personally identifiable information other than a credit card number or credit card security code.

**SEC. 4. METHODS OF NOTIFICATION.**

A business entity shall be in compliance with the requirements of this section if, with respect to the method of notification as required under section 2, the following requirements are met:

(1) INDIVIDUAL NOTIFICATION.—Notification to an individual is by one of the following means:

(A) Written notification to the last known home mailing address of the individual in the records of the business entity.

(B) Telephone notification to the individual personally.

(C) E-mail notification, if the individual has consented to receive such notification and the notification is consistent with the provisions permitting

electronic transmission of notifications under section 101 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001).

(2) MEDIA NOTIFICATION.—If the number of residents of a State whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person exceeds 5,000, notification is provided to media reasonably calculated to reach such individuals, such as major media outlets serving a State or jurisdiction.

**SEC. 5. CONTENT OF NOTIFICATION.**

The notification provided to individuals required by section 2 shall include, to the extent practicable, the following:

(1) A description of the categories of sensitive personally identifiable information that was, or is reasonably believed to have been, accessed or acquired by an unauthorized person.

(2) A toll-free number—

(A) that the individual may use to contact the business entity, or the agent of the business entity; and

(B) from which the individual may learn what types of sensitive personally identifiable information the business entity maintained about that individual.

(3) The toll-free contact telephone numbers and addresses for the major credit reporting agencies and the Commission.

(4) The name of the business entity that has a direct business relationship with the individual.

(5) Notwithstanding section 10, any information regarding victim protection assistance required by the State in which the individual resides.

**SEC. 6. COORDINATION OF NOTIFICATION WITH CREDIT REPORTING AGENCIES.**

(a) REQUIREMENT TO NOTIFY CREDIT REPORTING AGENCIES.—If a business entity is required to notify more than 5,000 individuals under section 2, the business entity shall also notify each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis (as defined in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)) of the timing and distribution of the notifications. Such notification shall be given to the consumer credit reporting agencies without

unreasonable delay and, if it will not delay notification to the affected individuals, prior to the distribution of notifications to the affected individuals.

(b) REASONABLE DELAY.—Reasonable delay under subsection (a) shall not exceed 30 days following the discovery of a security breach, except as provided in subsection (c) or (d) of section 2 (in which case, before the extended deadline), or unless the business entity providing notification can demonstrate to the Commission that additional time is reasonably necessary to determine the scope of the security breach, prevent further disclosures, conduct the risk assessment, restore the reasonable integrity of the data system, and provide notice to the breach notification entity. If the Commission determines that additional time is necessary, the Commission may extend the time period for notification for additional periods of up to 30 days each. Any such extension shall be provided in writing.

**SEC. 7. NOTIFICATION FOR LAW ENFORCEMENT AND OTHER PURPOSES.**

(a) NOTIFICATION TO LAW ENFORCEMENT AND NATIONAL SECURITY AUTHORITIES.—Any business entity shall notify the breach notification entity, and the breach notification entity shall promptly notify and provide that information to the United States Secret Service, the Federal Bureau of Investigation, and the Commission for civil law enforcement purposes, and shall make it available as appropriate to other Federal agencies for law enforcement, national security, or computer security purposes, if—

(1) the number of individuals whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person exceeds 5,000;

(2) the security breach involves a database, networked or integrated databases, or other data system containing the sensitive personally identifiable information of more than 500,000 individuals nationwide;

(3) the security breach involves databases owned by the Federal government; or

(4) the security breach involves primarily sensitive personally identifiable information of individuals known to the business entity to be employees and contractors of the Federal government involved in national security or law enforcement.

(b) REGULATIONS.—Not later than one year after the date of enactment of this Act, the Commission shall promulgate regulations (in accordance with section 553 of title 5, United States Code), in consultation with the Attorney General and the Secretary of Homeland Security, that describe what information is required to be included in the notification under subsection (a). In addition, the Commission shall, as necessary, promulgate regulations (in accordance with section 553 of title 5, United States

Code), in consultation with the Attorney General, to adjust the thresholds for notification to law enforcement and national security authorities under subsection (a) and to facilitate the purposes of this section.

(c) TIMING OF NOTIFICATION.—The notification required under this section shall be provided as promptly as practicable and at least 72 hours before notification of an individual pursuant to section 2 or ten days after discovery of the breach requiring notification, whichever comes first.

## SEC. 8. ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.

(a) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of this Act or a regulation promulgated under this Act shall be treated as a 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.—The Federal Trade Commission shall enforce this Act and the regulations promulgated under this Act 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 Act, except that the exceptions described in section 5(a)(2) of such Act (15 U.S.C. 45(a)(2)) shall not apply. Any business entity who violates this Act or a regulation promulgated under this Act shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act.

(c) FEDERAL COMMUNICATIONS COMMISSION.—In a case in which enforcement under this Act involves a business entity that is subject to the authority of the Federal Communications Commission, in enforcement actions by the Commission, the Commission shall consult with the Federal Communications Commission.

(d) CONSUMER FINANCIAL PROTECTION BUREAU.—In a case in which enforcement under this Act relates to financial information or information associated with the provision of a consumer financial product or service, in enforcement actions by the Commission, the Commission shall consult with the Consumer Financial Protection Bureau.

(e) CONSULTATION WITH THE ATTORNEY GENERAL REQUIRED.—The Commission shall consult with the Attorney General before opening an investigation. If the Attorney General determines that such an investigation would impede an ongoing criminal investigation or national security activity, the Commission may not open such investigation.

(f) REGULATIONS.—

(1) IN GENERAL.—The Commission may promulgate regulations, in addition to the regulations required pursuant to section 7(b), relating to the duties of the Commission under this Act, in accordance with section 553 of title 5, United States Code, as the Commission determines to be necessary to carry out this Act.

(2) FEDERAL COMMUNICATIONS COMMISSION.—With regard to a regulation promulgated under this section that relates to an entity subject to the authority of the Federal Communications Commission, the Commission may only promulgate such regulation after consultation with the Federal Communications Commission.

(3) CONSUMER FINANCIAL PROTECTION BUREAU.—With regard to a regulation promulgated under this section that relates to financial information or information associated with the provision of a consumer financial product or service, the Commission may only promulgate such regulation after consultation with the Consumer Financial Protection Bureau.

**SEC. 9. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

(a) IN GENERAL.—

(1) CIVIL ACTIONS.—In any case in which the attorney general of a State or an official or agency of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by an act or practice in violation of this Act or a regulation promulgated under this Act, the State, as parens patriae, may bring a civil action on behalf of the residents of the State in an appropriate State court or an appropriate district court of the United States to—

(A) enjoin that practice;

(B) enforce compliance with this Act; or

(C) impose civil penalties of not more than $1,000 per day per individual whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, up to a maximum of $1,000,000 per violation, unless such conduct is found to be willful or intentional.

(2) NOTICE.—Before filing an action under paragraph (1), the attorney general, official, or agency of the State involved shall provide to the Attorney General and the Commission—

(A) a written notice of the action; and

(B) a copy of the complaint for the action.

(3) ATTORNEY GENERAL CERTIFICATION.—An action may not be filed under paragraph (1) if the Attorney General determines that the filing would impede a criminal investigation or national security activity.

(b) AUTHORITY OF FEDERAL TRADE COMMISSION.—Upon receiving notice under subsection (a)(2), the Commission may—

(1) move to stay the action, pending the final disposition of a pending Federal proceeding or action;

(2) initiate an action in the appropriate United States district court under section 8 and move to consolidate all pending actions, including State actions, in such court;

(3) intervene in the action brought under subsection (a); or

(4) file petitions for appeal.

(c) PENDING PROCEEDINGS.—If the Commission has instituted a proceeding or action for a violation of this Act or any regulations promulgated under this Act, a State attorney general, official, or agency may not bring an action under this Act during the pendency of the Federal proceeding or action against any defendant named in such proceeding or action for any violation that is alleged in such proceeding or action.

(d) CONSTRUCTION.—For purposes of bringing any civil action under subsection (a), nothing in this Act shall be construed to prevent an attorney general, official, or agency of a State from exercising the powers conferred on such attorney general, official, or agency by the laws of that State to—

(1) conduct investigations;

(2) administer oaths or affirmations; or

(3) compel the attendance of witnesses or the production of documentary and other evidence.

(e) VENUE; SERVICE OF PROCESS.—

(1) VENUE.—Any action brought under subsection (a) may be brought in—

(A) the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code; or

(B) another court of competent jurisdiction.

(2) SERVICE OF PROCESS.—In an action brought under subsection (a), process may be served in any district in which the defendant—

(A) is an inhabitant; or

(B) may be found.

**SEC. 10. EFFECT ON STATE LAW.**

The provisions of this Act shall supersede any provision of the law of any State, or a political subdivision thereof, relating to notification by a business entity engaged in interstate commerce of a security breach, except as provided in section 5(5).

**SEC. 11. REPORTING ON SECURITY BREACHES.**

(a) REPORT REQUIRED ON NATIONAL SECURITY AND LAW ENFORCEMENT EXEMPTIONS.—Not later than 18 months after the date of enactment of this Act, and annually thereafter, the Director of the United States Secret Service and the Director of the Federal Bureau of Investigation shall submit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate on a report on the number and nature of security breaches subject to the national security and law enforcement exemptions under section 3(a).

(b) REPORT REQUIRED ON SAFE HARBOR EXEMPTIONS.—Not later than 18 months after the date of enactment of this Act, and annually thereafter, the Commission shall submit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report on the number and nature of the security breaches described in the notices filed by business entities invoking the risk assessment exemption under section 3(b) and the response of the Commission to such notices.

**SEC. 12. EXCLUDED BUSINESS ENTITIES.**

Nothing in this Act, or the regulations promulgated under this Act, shall apply to—

(1) business entities to the extent that such entities act as covered entities or business associates (as such terms are defined in section 13400 of the Health Information

Technology for Economic and Clinical Health Act (42 U.S.C. 17921) subject to section 13402 of such Act (42 U.S.C. 17932); and

(2) business entities to the extent that they act as vendors of personal health records (as such term is defined in section 13400 of such Act (42 U.S.C. 17921) and third-party service providers subject to section 13407 of such Act (42 U.S.C. 17937).

**SEC. 13. DEFINITIONS.**

IN THIS ACT:

(1) BREACH NOTIFICATION ENTITY.—The term "breach notification entity" means the Federal government entity designated pursuant to section 2(e).

(2) BUSINESS ENTITY.—The term "business entity" means any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture, whether or not established to make a profit.

(3) COMMISSION.—The term "Commission" means the Federal Trade Commission.

(4) CONSUMER FINANCIAL PRODUCT OR SERVICE.—The term "consumer financial product or service" has the meaning given that term in section 1002 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (12 U.S.C. 5481).

(5) DATA SYSTEM COMMUNICATION INFORMATION.—The term "data system communication information" means dialing, routing, addressing, or signaling information that identifies the origin, direction, destination, processing, transmission, or termination of each communication initiated, attempted, or received.

(6) DATE AND TIME.—The term "date and time" includes the date, time, and specification of the time zone offset from Coordinated Universal Time.

(7) FEDERAL AGENCY.—The term "Federal agency" has the meaning given the term "agency" in section 3502 of title 44, United States Code.

(8) INTELLIGENCE COMMUNITY.—The term "intelligence community" has the meaning given that term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(9) INTERNET ADDRESS.—The term "Internet address" means an Internet Protocol address as specified by the Internet Protocol version 4 or 6 protocol, or any successor protocol or any unique number for a specific host on the Internet.

(10) SECURITY BREACH.—

(A) IN GENERAL.—The term "security breach" means a compromise of the security, confidentiality, or integrity of, or the loss of, computerized data that results in, or there is a reasonable basis to conclude has resulted in—

(i) the unauthorized acquisition of sensitive personally identifiable information; or

(ii) access to sensitive personally identifiable information that is for an unauthorized purpose, or in excess of authorization.

(B) EXCLUSION.—The term "security breach" does not include any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an element of the intelligence community.

(11) SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.—The term "sensitive personally identifiable information" means any information or compilation of information, in electronic or digital form that includes one or more of the following:

(A) An individual's first and last name or first initial and last name in combination with any two of the following data elements:

(i) Home address or telephone number.

(ii) Mother's maiden name.

(iii)Month, day, and year of birth.

(B) A Social Security number (but not including only the last four digits of a Social Security number), driver's license number, passport number, or alien registration number or other Government-issued unique identification number.

(C) Unique biometric data such as a finger print, voice print, a retina or iris image, or any other unique physical representation.

(D) A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code.

(E) A user name or electronic mail address, in combination with a password or security question and answer that would permit access to an online account.

(F) Any combination of the following data elements:

(i) An individual's first and last name or first initial and last name.

(ii) A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code.

(iii) Any security code, access code, or password, or source code that could be used to generate such codes or passwords.

(12) MODIFIED DEFINITION BY RULEMAKING.—The Commission may, by rule promulgated under section 553 of title 5, United States Code, amend the definition of "sensitive personally identifiable information" to the extent that such amendment will accomplish the purposes of this Act. In amending the definition, the Commission may determine—

(A) that any particular combinations of information are sensitive personally identifiable information; or

(B) that any particular piece of information, on its own, is sensitive personally identifiable information.

**SEC. 14. EFFECTIVE DATE.**

This Act shall take effect 90 days after the date of enactment of this Act.

## 5.1 Codify Systemically Important Critical Infrastructure

This proposal codifies into law the concept of "systemically important critical infrastructure," whereby entities responsible for systemically critical systems and assets are granted special assistance from the U.S. government and shoulder additional security and information-sharing requirements befitting their unique status and importance.

---

**A BILL**

To codify the concept of 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,*

**SEC. 1. DEFINITIONS.—**

In this Act:

(1) CRITICAL INFRASTRUCTURE.—The term "critical infrastructure" has the meaning given that term in section 1016(e) of Public Law 107-56 (42 U.S.C. 5195c(e)).

(2) CYBER RISK.—The term "cybersecurity risk" has the meaning given the term in section 2209 of the Homeland Security Act of 2002.

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

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

(5) SECTOR-SPECIFIC AGENCY.—The term "Sector-Specific Agency" has the meaning given that term is section 2201 of the Homeland Security Act of 2002.

(6) SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE.—The term "systemically important critical infrastructure" means critical infrastructure that has been designated as systemically important critical infrastructure pursuant to the requirements of this Act.

**SEC. 2. CRITICAL INFRASTRUCTURE ASSESSMENT AND PRIORITIZATION.**

(a) IN GENERAL.—The Secretary, in consultation with entities that own or operate critical infrastructure, the Critical Infrastructure Partnership Advisory Council, and appropriate Information Sharing and Analysis Organizations, and in coordination

with the intelligence community, the Department of Defense, the Department of Commerce, Sector-Specific Agencies and other Federal agencies with responsibilities for regulating the security of entities that own or operate critical infrastructure shall—

(1) not later than one year after the date of enactment of this Act, and every four years thereafter, conduct and complete an assessment of the cybersecurity threats, vulnerabilities, risks, and probability of a catastrophic incident for all critical infrastructure sectors to determine which sectors, or subsets of sectors, are at the greatest risk, in order to guide the allocation of resources for the implementation of this Act; and

(2) following each assessment conducted pursuant to paragraph (1), and beginning with the highest priority sectors identified in such assessment, conduct, on a sector-by-sector basis, cyber risk assessments of critical infrastructure in a manner that—

(A) uses state-of-the art threat modeling, simulation, and analysis techniques;

(B) incorporates, as appropriate, any existing similar risk assessments; and

(C) considers—

(i) the actual or assessed threat, including consideration of adversary capabilities and intent, intrusion techniques, preparedness, target attractiveness, and deterrence capabilities;

(ii) the extent and likelihood of death, injury, or serious adverse effects to human health, and safety caused by damage or unauthorized access to critical infrastructure;

(iii) the threat to or impact on national security caused by damage or unauthorized access to critical infrastructure;

(iv) the extent to which damage or unauthorized access to critical infrastructure will disrupt the reliable operation of other critical infrastructure;

(v) the harm to the economy that would result from damage or unauthorized access to critical infrastructure;

(vi) the risk of national or regional catastrophic damage within the United States caused by damage or unauthorized access to critical infrastructure located outside the United States;

(vii) the overall preparedness and resilience of each sector against damage or unauthorized access to critical infrastructure, including the effectiveness of market forces at driving security innovation and secure practices; and

(viii) any other risk-based security factors appropriate and necessary to protect public health and safety, critical infrastructure, or national and economic security.

(b) INPUT OF OWNERS AND OPERATORS.—

(1) IN GENERAL.—The Secretary shall—

(A) establish a process under which entities that own or operate systemically important critical infrastructure and other relevant private sector experts provide input into the risk assessments conducted under this section; and

(B) seek and incorporate private sector expertise available through established public-private partnerships, including the Critical Infrastructure Partnership Advisory Council and appropriate Information Sharing and Analysis Organizations.

(2) PROTECTION OF INFORMATION.—Any information submitted pursuant to paragraph (1) shall be protected in accordance with section 107 of this Act.

(c) METHODOLOGIES FOR ASSESSING INFORMATION SECURITY RISK.—The Secretary and the Director of the National Institute of Standards and Technology, in consultation with entities that own or operate critical infrastructure and relevant private sector and academic experts, shall—

(1) develop repeatable, qualitative, and quantitative methodologies for assessing information security risk; or

(2) use repeatable, qualitative, and quantitative methodologies that are in existence on the date of enactment of this Act and make the methodologies publicly available.

(d) SUBMISSION OF RISK ASSESSMENTS.—

(1) IN GENERAL.—Not later than one year following the enactment of this Act and every four years thereafter, the Secretary shall submit each risk assessment conducted under this section to—

(A) the President;

(B) appropriate Federal departments and agencies; and

(C) the Majority and Minority Leaders of the Senate and the Speaker and Minority Leader of the House of Representatives.

(2) CLASSIFIED INFORMATION.—Each risk assessment submitted pursuant to paragraph (1) shall be in an unclassified form but may contain a classified annex.

**SEC. 3. PROCEDURE FOR DESIGNATION OF COVERED SYSTEMICALLY IMPORTANT SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE.**

(a) RESPONSIBILITY FOR DESIGNATION OF COVERED SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE.—

(1) PROCEDURES.—Not later than 18 months following the enactment of this Act, and every four years thereafter, the Secretary, in consultation with entities that own or operate critical infrastructure, the Critical Infrastructure Partnership Advisory Council, appropriate Information Sharing and Analysis Organizations, and other appropriate representatives of State and local governments, shall establish a procedure for the designation of critical infrastructure as systemically important critical infrastructure for the purposes of this Act.

(2) ELEMENTS.—In establishing the procedure under paragraph (1), the Secretary shall—

(A) prioritize the efforts of the Department based on the sector prioritization established under section 102(a)(1);

(B) incorporate, to the extent practicable, the input of entities that own or operate critical infrastructure, the Critical Infrastructure Partnership Advisory Council, appropriate Information Sharing and Analysis Organizations, and other appropriate representatives of the private sector and State and local governments;

(C) coordinate with the head of the Sector-Specific Agency and the head of any Federal department or agency with responsibilities for regulating the security of critical infrastructure;

(D) develop a mechanism for owners to submit information to assist the Secretary in making determinations under this section; and

(E) periodically, but not less often than every four years, review and update designations under this section.

(b) DESIGNATION OF SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE.—

(1) GUIDELINES FOR DESIGNATION.—In designating systemically important critical infrastructure for the purposes of this Act, the Secretary shall—

(A) designate systemically important critical infrastructure at the appropriate function, facility, system, or asset level;

(B) inform owners of the criteria used to identify systemically important critical infrastructure;

(C) only designate a function, facility, system, or asset as systemically important critical infrastructure if damage or unauthorized access to that system or asset could reasonably result in—

(i) the interruption of life-sustaining activities or services, including energy, water, transportation, emergency services, medical services, or food, sufficient to cause—

(I) a mass casualty event that includes an extraordinary number of fatalities; or

(II) mass evacuations with a prolonged absence;

(ii) catastrophic economic damage to the United States including—

(I) failure or substantial disruption of a United States financial market;

(II) unavailability or significant disruption of critical technology services, including related to telecommunications technology, cloud computing technology, and related information systems and technology infrastructure;

(III) incapacitation or sustained disruption of a transportation system; or

(IV) other systemic, long-term damage to the United States economy; or

(iii) severe degradation of defense, aerospace, military, national security or national security capabilities, including intelligence and defense functions; and

(D) consider the sector-by-sector risk assessments developed pursuant to section 102.

(2) LIMITATIONS.—The Secretary may not designate as systemically important critical infrastructure under this section—

(A) a system or asset based solely on activities protected by the First Amendment to the Constitution of the United States;

(B) an information technology product or service based solely on a finding that the product or service is capable of, or is actually, being used in systemically important critical infrastructure;

(C) a commercial information technology product, including hardware and software; or

(D) any service provided in support of a product specified in subparagraph (C), including installation services, maintenance services, repair services, training services, and any other services provided in support of the product.

(3) NOTIFICATION OF IDENTIFICATION OF SYSTEM OR ASSET.—Not later than 30 days after the Secretary designates a function, facility, system, or asset as systemically important critical infrastructure under this section, the Secretary shall notify the owner of each—

(A) facility, system, or asset that was designated and the basis for the designation; and

(B) facility, system, or asset that is covered by the designation of a function.

(4) SYSTEM OR ASSET NO LONGER COVERED AS SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE.—If the Secretary determines that any facility, system, or asset that was designated as systemically important critical infrastructure under this section no longer constitutes systemically important critical infrastructure, the Secretary shall promptly notify the owner of that facility, system, or asset of that determination.

(5) DEFINITION.—In this subsection, the term "damage" has the meaning given that term in section 1030(e) of title 18, United States Code.

(c) REDRESS.—

(1) IN GENERAL.—Subject to paragraphs (2) and (3), the Secretary shall develop a mechanism, consistent with subchapter II of chapter 5 of title 5, United States Code, for an owner notified under subsection (b)(3) or (4) to request that the Secretary review—

(A) the designation of a system or asset as covered systemically important critical infrastructure; or

(B) the determination that a system or asset no longer constitutes systemically important critical infrastructure; or

(2) APPEAL TO FEDERAL COURT.—A civil action seeking judicial review of a final agency action taken under the mechanism developed under paragraph (1) shall be filed in the United States District Court for the District of Columbia.

(3) COMPLIANCE.—An owner shall comply with the requirements of this Act relating to systemically important critical infrastructure until such time as the system or asset is no longer designated as systemically important critical infrastructure, based on—

(A) an appeal under paragraph (1);

(B) a determination of the Secretary unrelated to an appeal; or

(C) a final judgment entered in a civil action seeking judicial review brought in accordance with paragraph (2).

**SEC. 4. PERFORMANCE STANDARDS.—**

(a) IN GENERAL.—The Secretary, in coordination with each Sector-Specific Agency, and in consultation owners and operators of systemically important critical infrastructure, the Critical Infrastructure Partnership Advisory Council, and appropriate Information Sharing and Analysis Organizations, and in coordination with the Director of the National Security Agency, appropriate representatives from State and local governments, and other Federal agencies with responsibilities for regulating the security of covered systemically important critical infrastructure, shall identify or develop risk-based cybersecurity performance standards for systemically important critical infrastructure (referred to in this section as "performance standards") that—

(1) establish standards of responsibility for owners to remediate or mitigate identified cyber risks and any associated consequences identified under section 102(a) or otherwise;

(2) are structured into performance tiers that take into consideration—

(A) the size of the entity;

(B) resources available for security operations and compliance;

(C) whether the entity is publicly-owned, privately-owned, or a non-profit; and

(D) the maturity of the entity's security operations;

(3) take into consideration, with respect to the cyber risk—

(A) the extent and likelihood of death, injury, or serious adverse effects to human health and safety caused by damage or unauthorized access to systemically important critical infrastructure;

(B) the threat to or impact on national security caused by damage or unauthorized access to systemically important critical infrastructure;

(C) the extent to which damage or unauthorized access to systemically important critical infrastructure will disrupt the reliable operation of other systemically important critical infrastructure; and

(D) the harm to the economy that would result from damage or unauthorized access to systemically important critical infrastructure; and

(4) incorporate, to the greatest extent practicable, existing industry practices, standards, and guidelines.

(b) SECTOR-SPECIFIC PERFORMANCE STANDARDS.—The Secretary, with the concurrence of the relevant Sector-Specific Agency, may supplement the performance standards identified or established pursuant to subsection (a) on a sector-by-sector basis to take into account sector-specific risks, challenges, or security concerns.

## SEC. 5. SECURITY OF COVERED SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE.

(a) IN GENERAL.—Not later than one year after the date of enactment of this Act, the Secretary, in consultation with owners and operators, and the Critical

Infrastructure Partnership Advisory Council, and in coordination with Sector-Specific Agencies and other Federal agencies with responsibilities for regulating the security of systemically important critical infrastructure, shall promulgate regulations to enhance the security of systemically important critical infrastructure against cyber risks.

(b) RESPONSIBILITIES.—The regulations promulgated under this section shall establish procedures under which each owner of systemically important critical infrastructure is required—

(1) to select and implement the cybersecurity measures best suited to satisfy the risk-based cybersecurity performance requirements developed pursuant to section 104 of this Act;

(2) to notify the Secretary and each Federal agency with responsibilities for regulating the security of the owners systemically important critical infrastructure of the security measure or measures selected by an owner in accordance with subparagraph (A);

(3) to develop and update continuity of operations and cyber incident response plans;

(4) to report, consistent with the protections in section 107 of this Act, significant cyber incidents affecting the owner's systemically important critical infrastructure; and

(5) to certify, on an annual basis, in writing to the Secretary and the head of any Federal agency with responsibilities for regulating the security of the systemically important critical infrastructure that the owner has developed and effectively implemented security measures sufficient to satisfy the risk-based security performance requirements established under section 104 of this Act.

(c) ENFORCEMENT.—

(1) IN GENERAL.—The regulations promulgated under this section—

(A) shall impose civil penalties for any person who violates this section; and

(B) shall not confer upon any person, except the Federal agency with responsibilities for regulating the security of the systemically important critical infrastructure and the Secretary, a right of action against an owner or operator to enforce any provision of this section.

(2) ENFORCEMENT ACTIONS.—An action to enforce any regulation promulgated pursuant to this section shall be initiated by—

(A) the Federal agency with responsibility for regulating the security of the systemically important critical infrastructure, in consultation with the Secretary; or

(B) the Secretary, if —

(i) the systemically important critical infrastructure is not subject to regulation by another Federal agency;

(ii) the head of the Federal agency with responsibilities for regulating the security of the systemically important critical infrastructure requests the Secretary take such action; or

(iii) the Federal agency with responsibilities for regulating the security of the systemically important critical infrastructure fails to initiate such action after a request by the Secretary.

(d) SECURITY AND PERFORMANCE-BASED EXEMPTIONS.—

(1) IN GENERAL.—The regulations promulgated under this section shall include a process for an owner to demonstrate that—

(A) a covered facility, system, or asset is sufficiently secured against the risks identified in section 102; or

(B) compliance with risk-based performance requirements developed under section 104 would not substantially improve the security of the covered system or asset.

(2) EXEMPTION AUTHORITY.—Upon a determination by the Secretary that a covered system or asset is sufficiently secured against the risks identified in section 102, or that compliance with risk based performance standards developed under section 104 would not substantially improve the security of the system or asset, the Secretary shall exempt the owner from the requirements to select or implement cybersecurity measures or submit an annual certification required by this Act.

(3) RECURRENT DETERMINATION.—The Secretary shall require an owner that was exempted under paragraph (2) to demonstrate that the covered system or asset of the owner is sufficiently secured against the risks identified in section 102, or that compliance with risk-based performance standards

developed under section 104 would not substantially improve the security of the system or asset—

(A) not less than once every three years; or

(B) at any time, if the Secretary has reason to believe that the covered system or asset no longer meets the exemption qualifications under paragraph (2).

(e) OTHER ASSESSMENTS.—The regulations promulgated under this section shall establish procedures under which the Secretary—

(1) may perform cybersecurity assessments of selected systemically important critical infrastructure, in consultation with relevant agencies, based on—

(A) the specific cyber risks affecting or potentially affecting the information infrastructure of the specific system or asset constituting covered systemically important critical infrastructure;

(B) any reliable intelligence or other information indicating a cyber risk to the information infrastructure of the specific system or asset constituting covered systemically important critical infrastructure;

(C) actual knowledge or reasonable suspicion that an owner is not in compliance with risk-based security performance requirements established under section 104; or

(D) such other risk-based factors as identified by the Secretary;

(2) may use the resources of any relevant Federal agency with the concurrence of the head of such agency;

(3) to the extent practicable uses government and private sector information security assessment programs that were in existence on the date of enactment of this Act to conduct assessments; and

(4) provides copies of any Federal government assessments to the owner of the covered system or asset.

(f) ACCESS TO INFORMATION.—

(1) IN GENERAL.—For the purposes of an assessment conducted under paragraph (1) or (2) of subsection (e), an owner or operator shall provide an assessor any reasonable access necessary to complete the assessment.

(2) PROTECTION OF INFORMATION.—Information provided to the Secretary, the Secretary's designee, or any assessor during the course of an assessment under this section shall be protected from disclosure in accordance with section 107 of this Act.

## SEC. 6. DUPLICATIVE REQUIREMENTS.

(a) IN GENERAL.—The head of each agency with responsibilities for regulating the security of systemically important critical infrastructure shall coordinate with the Secretary on any activities that relate to the efforts of the agency regarding the cybersecurity and resilience to cyberattack of covered systemically important critical infrastructure, within or under the supervision of the agency.

(b) DUPLICATIVE REPORTING REQUIREMENTS.—

(1) IN GENERAL.—The Secretary shall coordinate with the head of any Federal agency with responsibilities for regulating the security of covered systemically important critical infrastructure to determine whether reporting requirements in effect on the date of enactment of this Act substantially fulfill any reporting requirements required by this Act.

(2) PRIOR REQUIRED REPORTS.—If the Secretary determines that a report that was required under a regulatory regime in existence on the date of enactment of this Act substantially satisfies a reporting requirement under this title, the Secretary shall accept such report and may not require an owner or operator to submit an alternate or modified report.

(3) COORDINATION.—The Secretary shall coordinate with the head of any Federal agency with responsibilities for regulating the security of systemically important critical infrastructure to eliminate any duplicate reporting or compliance requirements relating to the security or resiliency of systemically important critical infrastructure.

(c) REQUIREMENTS.—

(1) IN GENERAL.—To the extent that the head of any Federal agency with responsibilities for regulating the security of systemically important critical infrastructure has the authority to establish regulations, rules, or requirements or other required actions that are applicable to the security of systemically important critical infrastructure and covered systemically important critical infrastructure, the head of the agency shall—

(A) notify the Secretary in a timely fashion of the intent to establish the regulations, rules, requirements, or other required actions;

(B) coordinate with the Secretary to ensure that the regulations, rules, requirements, or other required actions are consistent with, and do not conflict or impede, the activities of the Secretary under this Act; and

(C) in coordination with the Secretary, ensure that the regulations, rules, requirements, or other required actions are implemented, as they relate to systemically important critical infrastructure, in accordance with subsection (a).

(2) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to provide additional authority for any Federal agency with responsibilities for regulating the security of systemically important critical infrastructure to establish standards or other measures that are applicable to the security of systemically important critical infrastructure not otherwise authorized by law.

**SEC. 7. PROTECTION OF INFORMATION.**

(a) DEFINITION.—In this section, the term "covered information"—

(1) means—

(A) any information that constitutes a privileged or confidential trade secret or commercial or financial transaction that is appropriately marked at the time it is provided by entities that own or operate systemically important critical infrastructure in sector-by-sector risk assessments conducted under section 102 of this Act;

(B) any information required to be submitted by owners and operators pursuant to section 105 of this Act; and

(C) any information submitted by State and local governments, private entities, and international partners of the United States regarding threats, vulnerabilities, risks, and incidents affecting—

(i) the Federal information infrastructure;

(ii) information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community; or

(iii)systemically important critical infrastructure; and

(2) does not include any information described under paragraph (1), if that information is submitted to—

(A) conceal violations of law, inefficiency, or administrative error;

(B) prevent embarrassment to a person, organization, or agency; or

(C) interfere with competition in the private sector.

(b) VOLUNTARILY SHARED SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE INFORMATION.—Covered information submitted in accordance with this section shall be treated as voluntarily shared systemically important critical infrastructure information under section 2224 of the Homeland Security Act, except that the requirement of such section 2224 that the information be voluntarily submitted, including the requirement for an express statement, shall not be required for protection of information under this section.

(c) GUIDELINES.—

(1) IN GENERAL.—Subject to paragraph (2), the Secretary shall develop and issue guidelines, in consultation with the Attorney General the Critical Infrastructure Partnership Advisory Council, and appropriate Information Sharing and Analysis Organizations, as necessary to implement this section.

(2) REQUIREMENTS.—The guidelines developed under this section shall—

(A) include provisions for the sharing of information among governmental and nongovernmental officials and entities in furtherance of carrying out the authorities and responsibilities of the Secretary pursuant to this Act;

(B) be consistent, to the maximum extent practicable, with policy guidance and implementation standards developed by the National Archives and Records Administration for controlled unclassified information, including with respect to marking, safeguarding, dissemination, and dispute resolution; and

(C) describe, with as much detail as practicable, the categories and type of information entities should voluntarily submit.

(d) RULES OF CONSTRUCTION.—Nothing in this section shall be construed to—

(1) limit or otherwise affect the right, ability, duty, or obligation of any entity to use or disclose any information of that entity, including in the conduct of any judicial or other proceeding;

(2) prevent the classification of information submitted under this section if that information meets the standards for classification under Executive Order 12958, or any successor thereto, or affect measures and controls relating to the protection of classified information as prescribed by Federal statute or under Executive Order 12958, or any successor thereto;

(3) limit the right of an individual to make any disclosure—

(A) protected or authorized under section 2302(b)(8) or 7211 of title 5, United States Code;

(B) to an appropriate official of information that the individual reasonably believes evidences a violation of any law, rule, or regulation, gross mismanagement, or substantial and specific danger to public health, safety, or security, and that is protected under any Federal or State law (other than those referenced in subparagraph (A)) that shields the disclosing individual against retaliation or discrimination for having made the disclosure if such disclosure is not specifically prohibited by law and if such information is not specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs; or

(C) to the Special Counsel, the Inspector General of an agency, or any other employee designated by the head of an agency to receive similar disclosures;

(4) prevent the Secretary from using information required to be submitted under this Act for enforcement of this title, including enforcement proceedings subject to appropriate safeguards;

(5) authorize information to be withheld from Congress, the Comptroller General, or the Inspector General of the Department;

(6) affect protections afforded to trade secrets under any other provision of law; or

(7) create a private right of action for enforcement of any provision of this section.

(e) AUDIT.—

(1) IN GENERAL.—Not later than one year after the date of enactment of this Act, the Inspector General of the Department shall conduct an audit of the

management of information submitted under this section and report the findings to appropriate committees of Congress.

(2) CONTENTS.—The audit under paragraph (1) shall include assessments of—

(A) whether the information is adequately safeguarded against inappropriate disclosure;

(B) the processes for marking and disseminating the information and resolving any disputes;

(C) how the information is used for the purposes of this section, and whether that use is effective;

(D) whether information sharing has been effective to fulfill the purposes of this section;

(E) whether the kinds of information submitted have been appropriate and useful, or overbroad or overly narrow;

(F) whether the information protections allow for adequate accountability and transparency of the regulatory, enforcement, and other aspects of implementing this title; and

(G) any other factors at the discretion of the Inspector General.

**SEC. 8. VOLUNTARY TECHNICAL ASSISTANCE.**

Subject to the availability of resources, and in accordance with applicable law relating to the protection of trade secrets, the Secretary shall provide voluntary technical assistance at the request of an owner or operator of systemically important critical infrastructure, to assist the owner or operator in meeting the requirements of section 105, including—

(a) implementing required security or emergency measures;

(b) restoring the systemically important critical infrastructure in the event of destruction or serious disruption: and

(c) developing emergency response plans.

**SEC. 9. EMERGENCY PLANNING.**

In partnership with owners and operators of systemically important critical infrastructure, the Secretary, in coordination with the heads of Sector-Specific Agencies and the heads of other Federal agencies with responsibilities for regulating the security of systemically

important critical infrastructure, shall exercise response and restoration plans, including plans required under section 105(b) to—

(a) assess performance and improve the capabilities and procedures of government and private sector entities to respond to a major cyber incident; and

(b) clarify specific roles, responsibilities, and authorities of government and private sector entities when responding to a major cyber incident.

## SEC. 10. INTERNATIONAL COOPERATION.

(a) IN GENERAL.—The Secretary, in coordination with the Secretary of State, shall—

(1) consistent with the protection of intelligence sources and methods and other sensitive matters, share information related to a cyber risk to critical infrastructure located outside the United States, the disruption of which could result in national or regional catastrophic damage within the United States, with—

(A) the owner or operator of such critical infrastructure; and

(B) the government of the country in which such critical infrastructure is located; and

(2) coordinate with the government of the country in which such critical infrastructure is located and, as appropriate, the owner or operator of the critical infrastructure, regarding the implementation of security measures or other measures to mitigate or remediate the cyber risks.

(b) INTERNATIONAL AGREEMENTS.—The Secretary, in coordination with the Secretary of State, shall perform the functions prescribed by this section consistent with applicable international agreements.

## SEC. 11. LIMITATION OF LIABILITY.

(a) IN GENERAL.—Except as provided in subsection (b), no cause of action shall lie in any court against the owner or operator of a systemically important critical infrastructure entity for damages directly caused by an incident related to a cyber risk identified under section 102, if the owner or operator—

(1) has implemented security measures, or a combination thereof, that satisfy the security performance requirements established under section 104;

(2) has submitted an annual certification as required by section 105(b)(1)(e), or been granted an exemption pursuant to section 105(e)(2); and

(3) is in substantial compliance with the appropriate risk-based cybersecurity performance requirements at the time of the incident related to that cyber risk.

(b) LIMITATION.—Paragraph (1) shall only apply to harm directly caused by the incident related to the cyber risk and shall not apply to damages caused by any additional or intervening acts or omissions by the owner or operator.

## SEC. 12. INTELLIGENCE SUPPORT TO SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE

(a) SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE CYBERSECURITY INTELLIGENCE NEEDS AND PRIORITIES.—

(1) IN GENERAL.—Not later than one year following the enactment of this Act, the Director of National Intelligence, in coordination with the Secretary and appropriate Sector-Specific Agencies shall establish a formal process to routinely provide intelligence support and indications and warning to systemically important critical infrastructure.

(2) PROCEDURES.—The Director of National Intelligence, in coordination with the Secretary shall establish methods and procedures —

(A) to identify the types of information needed to understand interdependence of systemically important critical infrastructure and areas where a nation-state adversary may target to cause widespread compromise or disruption, including—

(i) common technologies, including hardware and software, used within critical infrastructure sectors, within a geographic region, or across multiple critical infrastructure sectors;

(ii) critical lines of businesses, services, processes, and functions on which multiple critical infrastructure sectors are dependent;

(iii) specific technologies, components, materials, or resources on which a specific critical infrastructure sector, critical infrastructure within a specific geographic region, multiple critical infrastructure sectors, or critical infrastructure within multiple regions are dependent; and

(iv) Federal, State, local, tribal, or territorial government services, functions, and processes on which a specific critical

infrastructure sector, a specific geographic region, or multiple critical infrastructure sectors are dependent;

(B) to associate specific systemically important critical infrastructure entities with the information identified under subparagraph (A);

(C) to provide indications and warning to systemically important critical infrastructure entities identified under subparagraph (B) for nation-state adversary cyber operations relevant to information collected under subparagraph (A); and

(D) to identify any other intelligence gaps across systemically important critical infrastructure cybersecurity efforts.

(3) RECURRENT INPUT.— Not later than 30 days following the establishment of the process required pursuant to paragraph (1), and biennially thereafter, the Director of National Intelligence, in coordination with the Secretary of Homeland Security, shall solicit information from systemically important critical infrastructure utilizing the process established pursuant to this subsection.

(b) INTELLIGENCE COLLECTION.—Utilizing the information received through the process established pursuant to subsection (a), as well as existing intelligence information and processes, the Director of National Intelligence, in coordination with the Secretary and in consultation with Sector-Specific Agencies shall refocus information collection, analysis, and production activities as necessary to address identified gaps and mitigate threats to the cybersecurity of systemically important critical infrastructure of the United States.

(c) REQUIREMENT TO SHARE INTELLIGENCE INFORMATION WITH SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE.—

(1) IN GENERAL.—Not later than 30 days after discovery of information that potentially indicates a threat to a system identified in subsection (a)(2)(A) or to an identifiable systemically important critical infrastructure entity, the Director of National Intelligence shall share the appropriate intelligence information with the relevant owner or owners of systemically important critical infrastructure.

(2) EMERGENCY NOTIFICATION.—The Director of National Intelligence shall promptly share any intelligence information related to a systemically important critical infrastructure entity with such entity, if the Director determines that such information indicates an imminent threat to—

(A) a systemically important critical infrastructure system, asset, facility, service, or operation; or

(B) national security, economic security, or public health and safety.

(3) NATIONAL SECURITY EXEMPTIONS.—Notwithstanding paragraphs (1) or (2), the Director of National Intelligence may withhold intelligence information pertaining to a systemically important critical infrastructure entity if the Director, with the concurrence of the Secretary, determines that withholding such information is in the national security interest of the United States.

(d) REPORT TO CONGRESS.—Not later than 90 days following the completion of the evaluation pursuant to subsection (c), and annually thereafter, the Director of National Intelligence, in coordination with the Secretary, shall submit to the Select Committee on Intelligence and the Committee on Homeland Security and Governmental Affairs of the Senate and the Permanent Select Committee on Intelligence and the Committee on Homeland Security of the House of Representatives a report that—

(1) assesses how the information obtained from systemically important critical infrastructure is shaping intelligence collection activities;

(2) evaluates the success of the intelligence community in sharing relevant, actionable intelligence with systemically important critical infrastructure;

(3) lists any disclosures made and notifications withheld pursuant to subsection (b); and

(4) addresses any legislative or policy changes necessary to enable the intelligence community to increase sharing of actionable intelligence with systemically important critical infrastructure.

## SEC. 13. EXEMPTION AUTHORITY.

(a) IN GENERAL.—The President, in consultation with the Director of the Office of Management and Budget, may exempt a critical infrastructure sector, or a subset thereof, from regulation as systemically important critical infrastructure pursuant to this Act if the President determines that a Federal agency has sufficient specific regulatory requirements and enforcement mechanisms to effectively mitigate the risks, threats, and vulnerabilities identified under section 102.

(b) RECONSIDERATION.—The President may rescind any exemption under subsection (a) whenever the President determines that such rescission is in the interests of national security.

## SEC. 14. EFFECT ON OTHER LAWS.

This Act shall supersede any statute, provision of a statute, regulation, or rule of a State or political subdivision of a State that expressly requires comparable cybersecurity practices to protect systemically important critical infrastructure.

## 5.1.1 Increase Intelligence Support to the Private Sector

This proposal implements the Commission's recommendation to direct the executive branch to conduct a six-month comprehensive review of intelligence policies, procedures, and resources to identify and address key limitations in the ability of the intelligence community to provide intelligence support to the private sector.

---

**A BILL**

To improve the ability of the intelligence community to provide intelligence support to the private sector, and for other purposes.

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

**SEC. 1. REVIEW AND UPDATE INTELLIGENCE AUTHORITIES TO INCREASE INTELLIGENCE SUPPORT TO THE BROADER PRIVATE SECTOR.**

(a) REVIEW REQUIRED.—Not later than December 31, 2021, the Director of National Intelligence, in coordination with Director of the Cybersecurity and Infrastructure Security Agency and the Director of the National Security Agency, shall submit a comprehensive review of intelligence policies, procedures, and resources to the Select Committee on Intelligence and the Committee on Homeland Security and Governmental Affairs of the Senate and the Permanent Select Committee on Intelligence and the Committee on Homeland Security of the House of Representatives that identifies and addresses any legal or policy requirements that impede the ability of the intelligence community to support the private sector, and the Federal departments and agencies whose mission is to assist them in their cybersecurity and defense.

(b) ELEMENTS OF THE REVIEW.—The review developed pursuant to subsection (a) shall—

(1) identify and address limitations in collection on foreign adversary malicious cyber activity targeting domestic critical infrastructure;

(2) identify limitations in the ability of the intelligence community to share threat intelligence information with the private sector;

(3) review downgrade and declassification procedures for cybersecurity threat intelligence and assess options to improve the speed and timeliness of release;

(4) define criteria and procedures that would identify certain types of intelligence for expedited declassification and release;

(5) examine current and projected mission requirements of the National Security Agency's Cybersecurity Directorate to support other Federal departments and agencies and the private sector, including funding gaps;

(6) recommend budgetary changes needed to ensure that NSA meets expectations for increased support to other Federal department and agency cybersecurity efforts, including support to privately-sector critical infrastructure owners or operators;

(7) review cyber-related information-sharing consent processes, including consent to monitor agreements, and assess gaps and opportunities for greater standardization and simplification while ensuring privacy and civil liberty protections; and

(8) review existing statutes governing "national security systems", including National Security Directive 42, and assess the sufficiency of existing National Security Agency authorities to protect systems and assets that are critical to national security.

(c) SUBMISSION OF RECOMMENDATIONS.— The review required pursuant to subsection (a) shall include recommendations to address the gaps identified in the review.

(d) FORM OF REVIEW.—The review required pursuant to subsection (a) shall be submitted in unclassified form, but may include a classified annex.

## 5.1.2 Codify Processes for Identifying Private Sector Cyber Intelligence Needs and Priorities

This proposal implements the Commission's recommendation to direct ODNI and DHS, in consultation with relevant sector-specific agencies, to conduct a six-month review on how to establish a formal process to solicit and compile private-sector input to inform national intelligence priorities, collection requirements, and more focused U.S. intelligence support to private-sector cybersecurity operations.

---

**A BILL**

To codify processes for identifying private sector cyber intelligence needs and priorities, and for other purposes.

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

**SEC. 1. STRENGTHENING PROCESSES FOR IDENTIFYING CRITICAL INFRASTRUCTURE CYBERSECURITY INTELLIGENCE NEEDS AND PRIORITIES.**

(a) CRITICAL INFRASTRUCTURE CYBERSECURITY INTELLIGENCE NEEDS AND PRIORITIES.—

(1) IN GENERAL.—Not later than 180 days following the enactment of this Act, the Director of National Intelligence, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and appropriate Sector-Specific Agencies, as defined by section 2201 of the Homeland Security Act of 2002, shall establish a formal process to solicit and compile critical infrastructure input to inform national intelligence collection and analysis priorities.

(2) RECURRENT INPUT.— Not later than 30 days following the establishment of the process required pursuant to paragraph (1), and biennially thereafter, the Director of National Intelligence, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall solicit information from critical infrastructure utilizing the process established pursuant to paragraph (1).

(b) INTELLIGENCE NEEDS EVALUATION AND PLANNING.—Utilizing the information received through the process established pursuant to subsection (a), as well as existing intelligence information and processes, the Director of National

Intelligence, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall—

(1) identify common technologies or interdependencies that are likely to be targeted by nation-state adversaries;

(2) identify intelligence gaps across critical infrastructure cybersecurity efforts;

(3) identify and execute methods of empowering sector-specific agencies to—

(A) identify specific critical lines of businesses, technologies, and processes within their respective sectors; and

(B) coordinate directly with the intelligence community to convey specific information relevant to the operation of each sector; and

(4) refocus information collection and analysis activities, as necessary to address identified gaps and mitigate threats to the cybersecurity of critical infrastructure of the United States.

(c) REPORT TO CONGRESS.—Not later than 90 days following the completion of the evaluation pursuant to subsection (b), and annually thereafter, the Director of National Intelligence and the Director of the Cybersecurity and Infrastructure Security Agency shall submit to the Select Committee on Intelligence and the Committee on Homeland Security and Governmental Affairs of the Senate and the Permanent Select Committee on Intelligence and the Committee on Homeland Security of the House of Representatives a report that—

(1) assesses how the information obtained from critical infrastructure is shaping intelligence collection activities;

(2) evaluates the success of the intelligence community in sharing relevant, actionable intelligence with critical infrastructure; and

(3) addresses any legislative or policy changes necessary to enable the intelligence community to increase sharing of actionable intelligence with critical infrastructure.

(d) DEFINITION OF CRITICAL INFRASTRUCTURE.—The term "critical infrastructure" has the meaning given that term in section 1016(e) of Public Law 107-56 (42 U.S.C. 5195c(e)).

## 5.1.3 Grant Administrative Subpoena Authority to CISA

This proposal implements the Commission's recommendation to amend the Homeland Security Act of 2002 to protect United States critical infrastructure by ensuring that the Cybersecurity and Infrastructure Security Agency has the legal tools it needs to notify private and public sector entities put at risk by cybersecurity vulnerabilities in the networks and systems that control critical assets of the United States.

---

**A BILL**

To grant administrative subpoena authority to the Cybersecurity and Infrastructure Security Agency, and for other purposes.

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

**SEC. 1. SHORT TITLE.**

This Act may be cited as the "Cybersecurity Vulnerability Identification and Notification Act of 2019".

**SEC. 2. SUBPOENA AUTHORITY.**

(a) IN GENERAL.—Section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) is amended—

(1) in subsection (a)—

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

(B) by inserting after paragraph (5) the following: "(6) the term 'security vulnerability' has the meaning given that term in section 102(17) of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501(17));";

(2) in subsection (c)—

(A) in paragraph (10), by striking "and" at the end;

(B) in paragraph (11), by striking the period at the end and inserting "; and"; and

(C) by adding at the end the following: "(12) detecting, identifying, and receiving information about security vulnerabilities relating to critical

infrastructure in the information systems and devices of Federal and non-Federal entities for a cybersecurity purpose, as defined in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).”; and

(3) by adding at the end the following:

“(n) SUBPOENA AUTHORITY.—

“(1) DEFINITION.—In this subsection, the term ‘enterprise device or system’—

“(A) means a device or system commonly used to perform industrial, commercial, scientific, or governmental functions or processes that relate to critical infrastructure, including operational and industrial control systems, distributed control systems, and programmable logic controllers; and

“(B) does not include personal devices and systems, such as consumer mobile devices, home computers, residential wireless routers, or residential internet-enabled consumer devices.

“(2) AUTHORITY.—

“(A) IN GENERAL.—If the Director identifies a system connected to the internet with a specific security vulnerability and has reason to believe that the security vulnerability relates to critical infrastructure and affects an enterprise device or system owned or operated by a Federal or non-Federal entity, and the Director is unable to identify the entity at risk, the Director may issue a subpoena for the production of information necessary to identify and notify the entity at risk, in order to carry out a function authorized under subsection (c)(12).

“(B) LIMIT ON INFORMATION.—A subpoena issued under the authority under subparagraph (A) may only seek information in the categories set forth in subparagraphs (A), (B), (D), and (E) of section 2703(c)(2) of title 18, United States Code.

"(C) LIABILITY PROTECTIONS FOR DISCLOSING PROVIDERS.—The provisions of section 2703(e) of title 18, United States Code, shall apply to any subpoena issued under the authority under subparagraph (A).

"(3) COORDINATION.—

"(A) IN GENERAL.—If the Director decides to exercise the subpoena authority under this subsection, and in the interest of avoiding interference with ongoing law enforcement investigations, the Director shall coordinate the issuance of any such subpoena with the Department of Justice, including the Federal Bureau of Investigation, pursuant to inter-agency procedures which the Director, in coordination with the Attorney General, shall develop not later than 60 days after the date of enactment of this subsection.

"(B) CONTENTS.—The inter-agency procedures developed under this paragraph shall provide that a subpoena issued by the Director under this subsection shall be—

"(i) issued in order to carry out a function described in subsection (c)(12); and

"(ii) subject to the limitations under this subsection.

"(4) NONCOMPLIANCE.—If any person, partnership, corporation, association, or entity fails to comply with any duly served subpoena issued under this subsection, the Director may request that the Attorney General seek enforcement of the subpoena in any judicial district in which such person, partnership, corporation, association, or entity resides, is found, or transacts business.

"(5) NOTICE.—Not later than 7 days after the date on which the Director receives information obtained through a subpoena issued under this subsection, the Director shall notify the entity at risk identified by information obtained under the subpoena regarding the subpoena and the identified vulnerability.

"(6) AUTHENTICATION.—Any subpoena issued by the Director under this subsection shall be authenticated by the electronic signature of an authorized representative of the Agency or other comparable

symbol or process identifying the Agency as the source of the subpoena.

"(7) PROCEDURES.—Not later than 90 days after the date of enactment of this subsection, the Director shall establish internal procedures and associated training, applicable to employees and operations of the Agency, regarding subpoenas issued under this subsection, which shall address—

"(A) the protection of and restriction on dissemination of nonpublic information obtained through a subpoena issued under this subsection, including a requirement that the Agency shall not disseminate nonpublic information obtained through a subpoena issued under this subsection that identifies the party that is subject to the subpoena or the entity at risk identified by information obtained, unless—

"(i) the party or entity consents; or

"(ii) the Agency identifies or is notified of a cybersecurity incident involving the party or entity, which relates to the vulnerability which led to the issuance of the subpoena;

"(B) the restriction on the use of information obtained through the subpoena for a cybersecurity purpose, as defined in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501);

"(C) the retention and destruction of nonpublic information obtained through a subpoena issued under this subsection, including—

"(i) immediate destruction of information obtained through the subpoena that the Director determines is unrelated to critical infrastructure; and

"(ii) destruction of any personally identifiable information not later than 6 months after the date on which the Director receives information obtained through the subpoena, unless otherwise agreed to by the individual identified by the subpoena respondent;

"(D) the processes for providing notice to each party that is subject to the subpoena and each entity at risk identified by information obtained pursuant to a subpoena issued under this subsection; and

"(E) the processes and criteria for conducting critical infrastructure security risk assessments to determine whether a subpoena is necessary prior to being issued under this subsection.

"(8) REVIEW OF PROCEDURES.—Not later than one year after the date of enactment of this subsection, the Privacy Officer of the Agency shall—

"(A) review the procedures developed by the Director under paragraph (7) to ensure that—

"(i) the procedures are consistent with fair information practices; and

"(ii) the operations of the Agency comply with the procedures; and

"(B) notify the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives of the results of the review.

"(9) PUBLICATION OF INFORMATION.—Not later than 120 days after establishing the internal procedures under paragraph (7), the Director shall make publicly available information regarding the subpoena process under this subsection, including regarding—

"(A) the purpose for subpoenas issued under this subsection;

"(B) the subpoena process;

"(C) the criteria for the critical infrastructure security risk assessment conducted prior to issuing a subpoena;

"(D) policies and procedures on retention and sharing of data obtained by subpoena;

"(E) guidelines on how entities contacted by the Director may respond to notice of a subpoena; and

"(F) the procedures and policies of the Agency developed under paragraph (7).

"(10) ANNUAL REPORTS.—The Director shall annually submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report (which may include a classified annex but with the presumption of declassification) on the use of subpoenas under this subsection by the Director, which shall include—

"(A) a discussion of—

"(i) the effectiveness of the use of subpoenas to mitigate critical infrastructure security vulnerabilities;

"(ii) the critical infrastructure security risk assessment process conducted for subpoenas issued under this subsection;

"(iii) the number of subpoenas issued under this subsection by the Director during the preceding year;

"(iv) to the extent practicable, the number of vulnerable enterprise devices or systems mitigated under this subsection by the Agency during the preceding year; and

"(v) the number of entities notified by the Director under this subsection, and their response, during the previous year; and

"(B) for each subpoena issued under this subsection—

"(i) the source of the security vulnerability detected, identified, or received by the Director;

"(ii) the steps taken to identify the entity at risk prior to issuing the subpoena; and

"(iii) a description of the outcome of the subpoena, including discussion on the resolution or mitigation of the critical infrastructure security vulnerability.

"(11) PUBLICATION OF THE ANNUAL REPORTS.—The Director shall make a version of the annual report required by paragraph (10) publicly available, which shall, at a minimum, include the findings described in clause (iii), (iv) and (v) of subparagraph (A).".

## 5.2 Establish and Fund a Joint Collaborative Environment for Sharing and Fusing Threat Information

This proposal establishes a "Joint Collaborative Environment", a common, cloud-based environment in which the Federal government's unclassified and classified cyber threat information, malware forensics, and network data from monitoring programs are made commonly available for query and analysis—to the greatest extent possible. Given the complexity of such a program, this proposal only facilitates the initial design and does not extend into subsequent developments and broader applications.

---

**A BILL**

To establish a joint collaborative environment to enable greater cyber threat information sharing across government departments and agencies and between the public and private sector, and for other purposes.

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

**SEC. 1. JOINT COLLABORATIVE ENVIRONMENT.**

(a) IN GENERAL.—In coordination with the Cyber Threat Data Standards and Interoperability Council established pursuant to subsection (e), the Director of the Cybersecurity and Infrastructure Security Agency and the Director of the National Security Agency shall establish a joint, cloud-based, information sharing environment to—

(1) integrate the Federal government's unclassified and classified cyber threat intelligence, malware forensics, and data 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; and

(4) facilitate a whole-of-government, comprehensive understanding of the cyber threat facing the Federal government and national critical infrastructure networks.

(b) DEVELOPMENT.—

(1) INITIAL EVALUATION.—Not later than 180 days following the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency and the Director of the National Security Agency shall—

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

(B) evaluate all current programs, applications, or platforms of the Federal government that are intended to detect, identify, analyze, and monitor cyber threats against the United States or critical infrastructure.

(2) DESIGN.—Not later than one year following the evaluation required in paragraph (1), the Director of the Cybersecurity and Infrastructure Security Agency and the Director of the National Security Agency 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. At a minimum, this design shall—

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

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

(C) ensure accessibility by such Federal departments and agencies as the Director of the Cybersecurity and Infrastructure Security Agency and the Director for the National Security Agency determine 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; and

(H) anticipate the integration of new technologies and data streams, including data from Government-sponsored voluntary network sensors or network-monitoring programs for the private sector or for State, Local, tribal, and territorial governments.

(c) OPERATION.—The information sharing environment established pursuant to subsection (a) shall be jointly managed by—

(1) the Director of the Cybersecurity and Infrastructure Security Agency, who shall have responsibility for unclassified information and data streams; and

(2) the Director of the National Security Agency, who shall have responsibility for all classified information and data streams.

(d) POST-DEPLOYMENT ASSESSMENT.—Not later than two years following the deployment of the information sharing environment requirement by subsection (a), the Director of the Cybersecurity and Infrastructure Security Agency and the Director of the National Security Agency shall jointly assess the means by which the sharing environment can be expanded to include critical infrastructure information sharing organizations and, to the maximum extent practicable, begin the process of such expansion.

(e) CYBER THREAT DATA STANDARDS AND INTEROPERABILITY COUNCIL.—

(1) ESTABLISHMENT.—The President shall establish an interagency council, chaired by the Director of the Cybersecurity and Infrastructure Security Agency and the Director of the National Security Agency, to set data standards and requirements for program participation.

(2) OTHER MEMBERSHIP.—The President shall identify and appoint additional council members from Federal departments and agencies which oversee programs that generate, collect, or disseminate data or information related to the detection, identification, analysis, and monitoring of cyber threats.

(3) DATA STREAMS.—The council shall identify, designate, and periodically update, Federal programs required to participate in or be interoperable with the information sharing environment, including—

(A) government network-monitoring and intrusion detection programs;

(B) 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;

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

(D) malware forensics and reverse-engineering programs.

(4) DATA GOVERNANCE.—The council shall establish procedures and data governance structures, as necessary to protect sensitive data, comply with Federal regulations and statutes, and respect existing consent agreements with the private sector and other non-Federal entities.

(5) RECOMMENDATIONS.—As appropriate, the council, or the chairpersons thereof, shall recommend to the President budget and authorization changes necessary to ensure sufficient funding and authorities for the operation, expansion, adaptation, and security of the information sharing environment established pursuant to subsection (a).

(f) PRIVACY AND CIVIL LIBERTIES.—

(1) GUIDELINES OF ATTORNEY GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Attorney General shall, 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 title.

(2) FINAL GUIDELINES.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Attorney General shall, 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 Attorney General considers 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 title.

(B) PERIODIC REVIEW.—The Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers and private entities described in subparagraph (A), periodically, but not less frequently than once every two years, review the guidelines promulgated under subparagraph (A).

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

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

(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 title; 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 information 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 section 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 title; 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 the 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 title; and

(B) an assessment of the sufficiency of the policies, procedures, and guidelines established pursuant to section 105 in addressing concerns relating to privacy and civil liberties.

(2) BIENNIAL REPORT BY INSPECTORS GENERAL.—

(A) IN GENERAL.—Not later than two years after the date of the enactment of this Act and not less frequently than once every two 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 Inspectors General on Financial Oversight, 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 title.

(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 referred 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 title.

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

(h) CRITICAL INFRASTRUCTURE.—In this section, the term "critical infrastructure" has the meaning given that term in section 1016(e) of Public Law 107-56 (42 U.S.C. 5195c(e).

## 5.2.2 Pass a National Cyber Incident Reporting Law

This proposal implements the Commission's recommendation to pass a national cyber incident reporting law.

---

**A BILL**

To establish common standards and procedures for the prompt reporting of cybersecurity incidents suffered by private companies in the United States, and for other purposes.

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

**SEC. 1. MANDATORY REPORTING ENTITY DESCRIBED.**

For purposes of this Act, a 'mandatory reporting entity' is any entity that—

(1) owns, operates, support or maintains critical infrastructure, as that term is defined in section 5195c(e) of title 42, United States Code;

(2) meets the criteria established pursuant to subsection (b)(1); and

(3) has been notified of its reporting obligations consistent with the process established pursuant to subsection (b)(3).

**SEC. 2. CRITERIA AND PROCEDURES.**

The Secretary of Homeland Security, in consultation with the head of each [Sector-Specific Agency][Sector Risk Management Agency], shall establish and publish—

(1) criteria and procedures for identifying and designating mandatory reporting entities, including criteria related to—

(A) the likelihood of being targeted by a malicious cyber actor;

(B) consequences that disruption or compromise could cause to national security, economic security, or public health and safety; and

(C) maturity of security operations in detecting, investigating, and mitigating a cybersecurity incident.

(2) criteria for the types and thresholds of cyber incidents to be reported under this Act;

(3) processes for notifying entities that are designated pursuant to the process established under paragraph (1); and

(4) procedures to comply with reporting requirements pursuant to section 3 of this Act.

**SEC. 3. CYBERSECURITY INCIDENT REPORTING REQUIREMENTS.**

(a) IN GENERAL.—A mandatory reporting entity, identified pursuant to section 1, meets the requirements of this paragraph if, upon becoming aware of the possibility that a cybersecurity incident, including an incident involving ransomware, social engineering, malware, or unauthorized access, has occurred involving any critical infrastructure system or subsystem, the entity—

(1) promptly assesses whether or not such an incident occurred, and submits a notification meeting the requirements of subsection (b) to the Director of the Cybersecurity and Infrastructure Security Agency through the reporting processes established by the National Cybersecurity and Communications Integration Center as soon as practicable (but in no case later than 72 hours after the entity first becomes aware of the possibility that the incident occurred); and

(2) provides all appropriate updates to any notification submitted under paragraph (1).

(b) CONTENTS OF NOTIFICATION.—Each notification submitted under subparagraph (A) of paragraph (1) shall contain the following information with respect to any cybersecurity incident covered by the notification:

(1) The date, time, and time zone when the cybersecurity incident began, if known.

(2) The date, time, and time zone when the cybersecurity incident was detected.

(3) The date, time, and duration of the cybersecurity incident.

(4) The circumstances of the cybersecurity incident, including the specific critical infrastructure systems or subsystems believed to have been accessed and information acquired, if any.

(5) Any planned and implemented technical measures to respond to and recover from the incident.

(6) In the case of any notification which is an update to a prior notification, any additional material information relating to the incident, including technical data, as it becomes available.

## SEC. 3. EFFECT OF OTHER REPORTING.

A mandatory reporting entity shall not be considered to have satisfied the notification requirements of this Act by reporting information related to a cybersecurity incident to any person, agency or organization, including a law enforcement agency, other than to the Director of the Cybersecurity and Infrastructure Security Agency using the incident reporting procedures establish by the National Cybersecurity and Communications Integration Center.

## SEC. 4. DISCLOSURE, RETENTION, AND USE.

(a) AUTHORIZED ACTIVITIES.—Cybersecurity incidents and related reporting information provided to the Director of the Cybersecurity and Infrastructure Security Agency pursuant to this Act 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—

(1) a cybersecurity purpose;

(2) the purpose of identifying—

(A) a cybersecurity threat, including the source of such cybersecurity threat; or

(B) a security vulnerability;

(3) 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 a use of a weapon of mass destruction;

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

(5) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a threat described in paragraph (3) or any of the offenses listed in—

(A) sections 1028 through 1030 of title 18, United States Code (relating to fraud and identity theft);

(B) chapter 37 of such title (relating to espionage and censorship); and

(C) chapter 90 of such title (relating to protection of trade secrets).

(b) PROHIBITED ACTIVITIES.—Cybersecurity incidents and related reporting information provided to the Director of the Cybersecurity and Infrastructure Security Agency pursuant to this Act shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under subsection (a).

(c) PRIVACY AND CIVIL LIBERTIES.—Cybersecurity incidents and related reporting information provided to the Director of the Cybersecurity and Infrastructure Security Agency pursuant to this Act shall be retained, used, and disseminated by the Federal government—

(1) in a manner that protects from unauthorized use or disclosure any reporting information that may contain—

(A) personal information of a specific individual; or

(B) information that identifies a specific individual; and

(2) in a manner that protects the confidentiality of cybersecurity incident reporting information containing—

(A) personal information of a specific individual; or

(B) information that identifies a specific individual.

(d) FEDERAL REGULATORY AUTHORITY.—Cybersecurity incidents and related reporting information provided to the Director of the Cybersecurity and Infrastructure Security Agency pursuant to this Act shall not be used by any Federal, State, tribal, or local government to regulate, including an enforcement action, the lawful activities of any non-Federal entity.

**SEC. 5. LIMITATION ON REQUIRED REPORTING.**

(a) The Secretary may not set criteria or develop procedures pursuant to this Act that require a mandatory reporting entity, identified pursuant to section 1, to report on any cybersecurity incident unless such incident—

(1) has caused a loss in the confidentiality, integrity, or availability of proprietary, sensitive, or personal information;

(2) has caused a disruption or otherwise inhibited the ability of an entity to deliver services or conduct their primary business activity; or

(3) is a suspected nation-state attack.

## 5.2.3 Amend the Pen Register Trap and Trace Statute

This proposal reduces ambiguity and allows the private sector a broader range of defensive techniques by amending the Pen Register and Trap and Trace statute (18 U.S.C. § 3121) to help enable certain "active defense" activities.

---

**A BILL**

To amend statutes governing pen register trap and trace to better enable identification of malicious actors, and for other purposes.

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

**SEC. 1. PEN REGISTER TRAP AND TRACE ACTIVE DEFENSE.**

Section 3121 of chapter 206 of title 18, United States Code, is amended in subsection (b)—

(A) by striking "by a provider of electronic or wire communication service" in the matter preceding paragraph (1);

(B) in paragraph (1), by—

(i) inserting "by a provider of electronic or wire communication service" before "relating to the operation"; and

(ii) striking "; or" and inserting ";";

(C) in paragraph (2), by inserting "by a provider of electronic or wire communication service" before "to record the fact";

(D) in paragraph (3), by striking the period at the end and inserting "; or"; and

(E) by inserting at the end the following paragraph:

"(4) where such device is installed pursuant to a search warrant or used under a circumstance in which the contents of a communication may be intercepted under chapter 119 of this title.".

## 5.3 Establish an Integrated Cyber Center within CISA

This proposal implements the Commission's recommendation to directs the executive branch to strengthen a public-private, integrated cyber center within the Cybersecurity and Infrastructure Security Agency to support the critical infrastructure security and resilience mission and to conduct a one-year, comprehensive systems analysis review of Federal cyber and cybersecurity centers, including plans to develop and improve integration.

---

**A BILL**

To require a yearly review of integration of federal cyber and cybersecurity centers and an integrated cyber center within the Cybersecurity and Infrastructure Security Agency, and for other purposes.

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

**SEC. 1. REPORT ON THE CREATION OF AN INTEGRATED CYBER CENTER**

(a) REVIEW REQUIRED.—Not later than December 31, 2021, the [National Cyber Director] [the Department of Homeland Security], in coordination with the Department of Defense, the Department of Justice, the Federal Bureau of Investigation, the Office of the Director of National Intelligence, and the Privacy and Civil Liberties Oversight Board shall provide a report to Congress that details a comprehensive systems analysis review of Federal cyber and cybersecurity centers.

(b) ELEMENTS OF THE REVIEW.—The review developed pursuant to subsection (a) shall—

(1) identify continuing gaps and shortcomings in the Cybersecurity and Infrastructure Security Agency's current capacity, structure, funding, and integration of its work with Sector-Specific Agencies that prevent it from fulfilling its role as the central coordinator among Federal centers for critical infrastructure cybersecurity and resilience;

(2) identify facility needs for the Cybersecurity and Infrastructure Security Agency to adequately host personnel, maintain sensitive compartmented information facilities, and other resources to fulfill its mission of being the primary coordinating body charged with forging whole-of-government, public-private collaboration in cybersecurity (i.e. establish and maintain an integrated cyber center);

(3) assess the resources, funding, and personnel required for Cybersecurity and Infrastructure Security Agency to fulfill gaps and responsibilities identified pursuant to the review conducted pursuant to this section;

(4) assess continuing gaps and limitations in its ability to provide for greater centralization of public-private cybersecurity efforts;

(5) assess areas where existing Federal cyber centers, or portions of a center's mission, would benefit from greater integration or collocation to support cybersecurity collaboration with critical infrastructure, to include but not limited to the—

(A) National Security Agency's Cyber Threat Operations Center;

(B) Cyber Command's Joint Operations Center;

(C) Office of the Director of National Intelligence's Cyber Threat Intelligence Integration Center;

(D) Federal Bureau of Investigation's National Cyber Investigative Joint Task Force;

(E) Department of Defense's Defense Cyber Crime Center; and

(F) Office of the Director of National Intelligence's Intelligence Community Security Coordination Center;

(6) identify and acknowledge continuing gaps and shortcomings in associated capacity and funding of the Federal Bureau of Investigation and the Office of the Director of National Intelligence, identify methods to better integrate efforts with the Cybersecurity and Infrastructure Security Agency in support of the mission to ensure the security and resilience of critical infrastructure, and identify where Federal agencies have distinct statutory authorities best kept distinct and separate from these efforts;

(7) identify continuing gaps and opportunities for greater integration of National Security Agency's Cybersecurity Directorate with the Cybersecurity and Infrastructure Security Agency, other Federal cyber centers, and, as needed, the private sector in its role of securing national security systems;

(8) identify lessons from the United Kingdom's National Cybersecurity Center model to determine whether an integrated cyber center within the Cybersecurity and Infrastructure Security Agency should be similarly organized into two environments: an unclassified side and a classified side

with appropriate support from National Security Agency's Cybersecurity Directorate;

(9) recommend procedures and criteria for increasing and expanding the participation and integration of public- and private-sector personnel into U.S. government cyber defense and security efforts, to include continuing limitations or hurdles in the security clearance program for private sector partners and in integrating private sector partners into a Cybersecurity and Infrastructure Security Agency integrated cyber center; and

(10) in consultation with the Privacy and Civil Liberties Oversight Board, identify and assess potential risks to privacy and civil liberties posed by the creation of an integrated cyber center and recommend procedures and criteria for mitigating said risks.

(c) ANNUAL REVIEWS.—Upon submitting the initial review pursuant to subsection (a), the [National Cyber Director] [the Department of Homeland Security] shall conduct an annual review thereafter, providing a yearly report, not later than December 31 of each year, to Congress on the status of its efforts, any revised findings or additional resources or authorities required, and its progress in addressing the areas identified in the initial review.

# 5.4 Create a Joint Cyber Planning Office

This proposal implements the Commission's recommendation to create a Joint Cyber Planning Office in the Cybersecurity and Infrastructure Security Agency to facilitate comprehensive planning of defensive, non-intelligence cybersecurity campaigns across agencies and to integrate these planning efforts with the private sector. In this section, the term "Agency" refers to the Cybersecurity and Infrastructure Security Agency. If 1.3 National Cyber Director is adopted as Section 2215 then this would become Section 2216.

---

**A BILL**

To establish a Joint Cyber Planning Office within the Cybersecurity and Infrastructure Security Agency to facilitate comprehensive planning of defensive, non-intelligence cybersecurity campaigns across agencies and to integrate these planning efforts with the private sector, and for other purposes.

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

**SEC. 1. ESTABLISHMENT OF THE JOINT CYBER PLANNING OFFICE**

The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

(1) by inserting after section 2214 the following new section:

"**SEC. 2215. JOINT CYBER PLANNING OFFICE**.

"(a) ESTABLISHMENT OF OFFICE.—There is established in the Agency an office for joint cyber planning (referred to in this section as the 'Office') to carry out certain responsibilities of the Secretary. The Office shall be headed by a Director of Joint Cyber Planning.. The Office shall be located in the Agency.

"(b) MISSION.—The Office shall lead Government-wide and public-private planning for cyber defense campaigns, including the development of a set of coordinated actions to respond to and recover from significant cyber incidents or limit, mitigate, or defend against coordinated, malicious cyber campaigns that pose a potential risk to critical infrastructure of the United States and broader national interests..

"(c) PLANNING AND EXECUTION.—In leading the development of Government-wide and public-private plans for cyber defense campaigns pursuant to subsection (b), the Director of Joint Cyber Planning shall—

"(1) establish coordinated and deliberate processes and procedures across relevant Federal departments and agencies, accounting for all participating Federal agency cyber capabilities and authorities;

"(2) ensure that plans are, to the greatest extent practicable, developed in collaboration with relevant public- and private-sector entities, particularly in areas where such entities have comparative advantages in limiting, mitigating, or defending against a significant cyber incident or coordinated, malicious cyber campaign;

"(3) ensure that plans are responsive to potential adversary activity conducted in response to U.S. offensive cyber operations.

"(4) in order to inform and facilitate exercises of such plans, develop and model scenarios based on an understanding of adversary threats, critical infrastructure vulnerability, and potential consequences of disruption or compromise;

"(5) coordinate with and, as necessary, support relevant Federal agencies in the establishment of procedures, development of additional plans, including for offensive and intelligence activities in support of cyber defense campaign plans, and procurement of authorizations necessary for the rapid execution of plans once a significant cyber incident or malicious cyber campaign has been identified; and

"(6) support the Department and other Federal agencies, as appropriate, in coordination and execution of plans developed pursuant to this section.

"(d) COMPOSITION.—The Office shall be composed of a central planning staff and—

"(1) a central planning staff;

"(2) appropriate representatives of Federal entities, including—

"(A) the Department of Defense;

"(B) the National Security Agency;

"(C) the Federal Bureau of Investigation;

"(D) the Federal Emergency Management Agency; and

"(E) the Office of the Director of National Intelligence; and

"(3) appropriate representatives of non-Federal entities, such as—

"(A) State, local, and tribal governments;

"(B) information sharing and analysis organizations, including information sharing and analysis centers;

"(C) owners and operators of critical information systems; and

"(D) private entities; and

"(3) other appropriate representatives or entities, as determined by the Secretary.

"(e) INTERAGENCY AGREEMENTS.—The Secretary and the head of a Federal agency described in subsection (d) may enter into agreements for the purpose of detailing personnel on a reimbursable or non-reimbursable basis.

"(f) INFORMATION PROTECTION.—Information provided to the Office by a private entity shall be deemed to have been shared pursuant to section 103(c) of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1503(c)) and shall receive the protections and exemptions provided in such Act.

"(g) FUNDS.—There are authorized to be appropriated $15,000,000 to the Director of Joint Cyber Planning to carry out this section.

"(h) DEFINITIONS.—In this section:

"(1) CRITICAL INFRASTRUCTURE—The term 'critical infrastructure' means a physical or cyber system or asset that are so vital to the United States that the incapacity or destruction of such system or asset would have a debilitating impact on the physical or economic security of the United States or on public health or safety.

"(2) CYBER DEFENSE CAMPAIGN.—The term 'cyber defense campaign' means a set of coordinated actions to respond to and recover from a significant cyber incident or limit, mitigate, or defend against a coordinated, malicious cyber campaign targeting critical infrastructure in the United States.

"(3) SIGNIFICANT CYBER INCIDENT—The term 'significant cyber incident' means an incident that is, or group of related cyber incidents that together are, reasonably likely to result in significant harm to the national security, foreign policy, or economic health or financial stability of the United States"; and

(2) in the table of contents, by inserting after the item relating to section 2214 the following new item:

"Sec .2215. Joint Cyber Planning Office"

## 5.4.1 Institutionalize Department of Defense Participation in Public-Private Cybersecurity Initiatives

This proposal implements the Commission's recommendation to assess the impact of the current Pathfinder initiative, prospects for making existing Pathfinder pilots more robust, and whether and how to expand Pathfinder or similar models of public-private collaboration to other critical infrastructure sectors, particularly systemically important critical infrastructure. Developing institutional support for Pathfinder-type initiatives not only creates opportunities for increased collaboration across critical sectors, as prioritized by Federal departments and agencies, but will also buttress and accelerate nascent efforts and increase their chances of success.

---

**A BILL**

To assess the impact and potential for expansion of the Pathfinder program and similar initiatives intended to enhance public-private cooperation on cybersecurity matters, and for other purposes.

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

**SEC. 1. ASSESSING PRIVATE-PUBLIC COLLABORATION IN CYBERSECURITY.**

(a) REQUIREMENT.—The Secretary of Defense in coordination with the Secretary of the Department of Homeland Security shall, not later than December 31, 2021, —

(1) conduct a comprehensive review and assessment of any ongoing public-private collaborative initiatives involving the Department of Defense, the Department of Homeland Security, and the private sector related to cybersecurity and defense of critical infrastructure, including—

(A) the United States Cyber Command's Pathfinder initiative and any derivative initiative;

(B) an assessment of the Department of Defense's support to and integration with existing Federal cybersecurity centers and organizations; and

(C) an assessment of comparable initiatives led by other Federal departments or agencies that support long-term public-private cybersecurity collaboration; and

(2) make recommendations for improvements and the requirements and resources necessary to institutionalize and strengthen these programs identified in the assessments in subsection (1).

(b) REPORT.—

(1) IN GENERAL.—The Secretary shall submit to the Committees on Armed Services and Homeland Security and Governmental Affairs of the Senate and the Committees on Armed Services and Homeland Security of the House of Representatives a report on the assessment and recommendations developed pursuant to subsection (a).

(2) FORM OF REPORT.—The report under paragraph (1) may be submitted in unclassified form or classified form as necessary.

# 6.1 & 6.1.3 Perform a CMF Force Structure Assessment and Define Authorities for Cyber Operations

These amendments to the Cyber Posture Review (first introduced in the FY2018 NDAA in Section 1644) will implement the Commission's recommendations to address the rapidly changing strategic environment. To enable support for a more streamlined decision-making process, and flexible and rapid maneuver, the "Elements of Review" section is amended to include analysis and recommendations for the conditions under which further delegation of cyber-related authorities is appropriate to U.S. Cyber Command, as well as to other DoD components. The "Elements of Review" section is also amended to direct the Department of Defense to conduct a force structure assessment of the U.S. Cyber Command's Cyber Mission Force in light of growing mission requirements and expectations. These assessments are crucial for steady and consistent planning of the force.

---

**A BILL**

To augment the Cyber Posture Review to ensure U.S. Cyber Command is adequately staffed and resourced in light of growing mission requirements and expectations, and for other purposes.

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

**SEC. 1. CYBER POSTURE REVIEW.**

(a) Section 1644 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115-91) is amended—

(1) in subsection (c)—

(A) in paragraph (2), by inserting "and partners" following "allies";

(B) by striking paragraph (3) and inserting the following new paragraph:

"(3) A review of the law, policies, and authorities relating to, and necessary for the United States to maintain a safe, reliable, and credible cyber posture for defending against and responding to cyberattacks and for deterrence in cyberspace, including—

"(A) analysis and recommendations for the conditions under which further delegation of cyber-related authorities, including information warfare authorities, to Cyber Command is appropriate; and

"(B) an evaluation of the adequacy of mission authorities for all Department of Defense cyber-related military departments and defense agencies, directorates, centers and commands.";

(C) by redesignating paragraphs (9) through (11) as paragraphs (10) through (12), respectively; and

(D) by striking paragraph (8) and inserting the following new paragraphs:

"(8) A comprehensive force structure assessment of the Department's Cyber Mission Force for the posture review period, including—

"(A) a determination of the appropriate size and composition of the Cyber Mission Force to accomplish the Department's mission requirements;

"(B) whether the Cyber Mission Force is appropriately matched to the prioritization of threats in the cyber domain; and

"(C) whether the Cyber Mission Force has adequate resources to sustain the Department's responsibilities in cyberspace, including—

"(i) personnel;

"(ii) equipment; and

"(iii) funding.

"(9) An assessment of the resource implications for the National Security Agency and other relevant intelligence community organizations in their combat support agency roles to the Cyber Mission Force.".

## 6.1.1 Create a Major Force Program Funding Category for U.S. Cyber Command

To enhance the acquisition flexibility and agility of U.S. Cyber Command, Congress should direct in the FY2021 National Defense Authorization Act that the Department of Defense (DoD) create a Major Force Program (MFP) category for the training, manning, and equipping of U.S. Cyber Command. According to Section 238 of title 10 U.S. Code, the DoD was required to submit to Congress a budget justification display that included an MFP category for the Cyber Mission Force. However, this law was enacted in 2014, before U.S. Cyber Command was elevated to a unified combatant command. Furthermore, the reporting requirement for this section is due to terminate on December 31, 2021. Finally, Section 807 of the FY2016 NDAA granted limited acquisition authorities to U.S. Cyber Command. Similar to Section 238 of title 10 U.S. Code, this acquisition authority terminates in 2021. Therefore, there is a need for an MFP for U.S. Cyber Command. This would be analogous to the MFP funding category for U.S. Special Operations Command, which was created to support comparable needs for operational adaptability.

---

**SEC. 1. BUDGETING AND ACCOUNTING FOR U.S. CYBER COMMAND.**

(a) Section 167b. of Chapter 6 of title 10 United States Code, is amended by adding at the end of the following new subsections:

"(f) MAJOR FORCE PROGRAM CATEGORY.—The Secretary of Defense shall create for United States Cyber Command a major force program category for the Five-Year Defense Plan of the Department of Defense for the training, manning, and equipping of United States Cyber Command. The Deputy Assistant Secretary of Defense for Cyber Policy, with the advice and assistance of the commander of United States Cyber Command, shall provide overall supervision of the preparation and justification of program recommendations and budget proposals to be included in such major force program category.

"(g) PROGRAM AND BUDGET EXECUTION.—To the extent that there is authority to revise programs and budgets approved by Congress for United States Cyber Command, such authority may be exercised only by the Secretary of Defense, after consulting with the commander of United States Cyber Command.".

## 6.1.7 Assess the Establishment of a Military Cyber Reserve

This proposal implements the Commission's recommendation to assess the need for, and requirements of, a military cyber reserve (a "cyber reserve force" in legislative language), its possible composition, and its structure. The purpose of this assessment is to ensure the Department of Defense is prepared to mobilize a surge capacity in times of crisis or conflict. It will assess how different types of reserve models, including traditional uniformed reserve models, as well as non-traditional civilian and uniformed reserve models, could address broader talent management issues. The intent is for this particular assessment is to evaluate a uniformed military reserve that does not contain the same kinds of drilling, grooming, or physical expertise requirements as a traditional uniformed reserve. This intent is the same for the assessment of a civilian reserve force. This legislation will also include an evaluation of mechanisms to recruit talented people from the private sector during times of crisis, as well as recruiting and retaining civilian talent with no prior military expertise that are interested in serving.

---

**A BILL**

To direct the Department of Defense to assess the establishment of a military cyber reserve force, and for other purposes.

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

**SEC. 1. ASSESSING THE NECESSITY, COMPOSITION, AND REQUIREMENTS OF A CYBER RESERVE FORCE.**

(a) REQUIREMENT.—In order to effectively respond to a cybersecurity incident that requires a capable surge capacity and enables the Department of Defense to draw on cyber talent that currently resides in the military and the private sector, the Secretary of Defense shall, not later than December 31, 2021,—

(1) assess the capabilities and deficiencies in military and civilian personnel cybersecurity expertise within the Department;

(2) assess the necessity of establishing a voluntary cyber reserve force;

(3) assess personnel, funding requirements, and composition of a voluntary cyber reserve force;

(4) assess alternative models for establishing a voluntary cyber reserve force, including—

(A) traditional uniformed military reserve component;

(B) non-traditional, in relation to drilling and other requirements such as grooming and physical fitness, uniformed military reserve component; and

(C) non-traditional civilian cyber reserve options;

(5) assess the impact a uniformed military cyber reserve would have on Active Duty and existing Reserve forces, including—

(A) recruiting;

(B) promotion; and

(C) retention; and

(6) assess the impact of drawing a voluntary civilian cyber reserve from the private sector.

(b) REPORT.—

(1) IN GENERAL.— The Secretary shall submit to the congressional defense committees a report on the assessment and recommendations developed pursuant to subsection (a).

(2) FORM OF REPORT.— The report under paragraph (1) may be submitted in unclassified form or classified form as necessary.

## 6.2.a Conduct Cybersecurity Assessments Across NC3

This amendment to Section 1651 of the FY2018 National Defense Authorization Act (NDAA) implements the Commission's recommendation to require the Department of Defense to conduct an annual cybersecurity vulnerability assessment of all segments of the nuclear command and control system. Most importantly, rather than focusing solely on mission assurance, as Section 1651 did, this amendment will broaden the assessment to include quality assurance and the active identification of cyber vulnerabilities of each segment of the nuclear command and control that requires mitigation. This amendment will also call for an assessment of a program to seek, identify, and mitigate cybersecurity threats and vulnerabilities on nuclear command and control systems.

---

**A BILL**

To require the Department of Defense to conduct an annual cybersecurity vulnerability assessment of all segments of the nuclear command and control system, and for other purposes.

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

**SEC. 1. ANNUAL ASSESSMENT OF CYBER RESILIENCY OF NUCLEAR COMMAND AND CONTROL SYSTEM.**

Chapter 24 of title 10, United States Code, is amended—

(1) in section 499—

(A) by striking the section title and inserting the following:

"§ 499. Annual assessment of cyber vulnerability and resiliency of nuclear command and control system";

(B) in subsection (a), by inserting "vulnerability and" before "resiliency";

(C) in subsection (b)—

(i) in paragraph (1), by striking "and" after "potential threat;";

(ii) by redesignating paragraph (2) as paragraph (4); and

(iii)by inserting after paragraph (1) the following new paragraphs:

"(2) Conduct an assessment of the cyber vulnerabilities of all segments of the nuclear command and control system to ensure these systems are secure from cyberattacks from the Russian Federation, the People's Republic of China, or any other country or entity the Commanders identify as a potential threat;

"(3) Conduct an assessment on the need to establish a program to actively seek and identify cybersecurity threats and vulnerabilities on the nuclear command and control system led by the National Security Agency's Strategic Cybersecurity Program and the United States Cyber Command; and"; and

(D) in subparagraph (c)(1)(C), by inserting "quality and" before "mission assurance".

(2) in the table of contents, by striking the item relating to section 499 and inserting the following:

"Sec. 499 Annual assessment of cyber vulnerability and resiliency of nuclear command and control system".

## 6.2.b Conduct Cybersecurity Assessment of Weapon Systems

This proposal amends Section 1647 of the National Defense Authorization Act (NDAA) (Public Law 114-92), which was amended in the FY2020 NDAA (Section 1633). This implements the Commission's recommendation to ensure the Department of Defense (DoD) presents a plan to annually assess major weapon system vulnerabilities. This proposal also calls for an after-action report that includes current and planned efforts to address cyber vulnerabilities of interdependent and networked weapon systems in broader mission areas, with an intent to gain mission assurance of these platforms. Finally, this amendment calls for a plan for comprehensive annual assessments of major weapon systems, taking into account lessons learned from Section 1651 of the FY2018 NDAA.

---

**SEC. 1. EVALUATION OF CYBER VULNERABILITIES OF MAJOR WEAPON SYSTEMS OF THE DEPARTMENT OF DEFENSE.**

Section 1647 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114-92) is amended by adding at the end the following new subsections:

"(h) AFTER-ACTION REPORT.— Not later than December 31, 2021, the Secretary, acting through the Under Secretary of Defense for Acquisition and Sustainment, shall provide an after-action report to the congressional defense committees upon receipt of the results of the evaluation of the cyber vulnerabilities of each major weapon system of the Department under this section. Such report may be classified, if necessary, and shall include an identification of current and planned efforts to address cyber vulnerabilities of major weapon systems that includes vulnerabilities across networked weapon systems in broader mission areas, with a focus on the risk of older weapon systems integrating with new weapon systems across missions.

"(i) PLAN REQUIRED.—Not later than December 31, 2021, the Secretary of Defense shall develop a comprehensive plan for the annual assessment of cyber vulnerabilities of major weapon systems of the Department of Defense, sharing lessons learned and best practices from the annual assessment of cyber resiliency of nuclear command and control system required in Section 1651 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115-91).".

## 6.2.1 Require DIB Participation in a Threat Intelligence Program

This proposal implements the Commission's recommendation to require the companies that make up the defense industrial base (DIB), as part of the terms of their contract with the Department of Defense (DoD), to participate in a threat intelligence sharing program that would be housed at the DoD component level. The DoD lacks a complete view of its supply chain. Therefore, prime contractors will be incentivized to disclose their subcontractors to DoD. Furthermore, drawing on DoD's Cyber Maturity Model Certification (CMMC) regulation, the requirements associated with participation in a threat intelligence sharing program will be tied to a firm's level of maturity. This proposal does not expand to the whole supply chain, due to the increasing risk of higher resistance to making such an action mandatory. The DIB is a unique sector due to its importance to national security.

---

**A BILL**

To establish a threat intelligence program facilitating information sharing between the Department of Defense and the private companies that make up the defense industrial base, and for other purposes.

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

**SEC. 1. DEFENSE INDUSTRIAL BASE PARTICIPATION IN A THREAT INTELLIGENCE SHARING PROGRAM.**

(a) DEFENSE INDUSTRIAL BASE.—In this Act, the term "defense industrial base" means the worldwide industrial complex with capabilities to perform research and development, design, produce, deliver, and maintain military weapon systems, subsystems, components, or parts to meet military requirements.

(b) DEFENSE INDUSTRIAL BASE THREAT INTELLIGENCE PROGRAM.—

(1) IN GENERAL.—The Secretary of Defense shall establish a threat intelligence sharing program to share threat intelligence with, and obtain threat intelligence from, the defense industrial base.

(2) PROGRAM REQUIREMENTS.—At a minimum, the Secretary shall ensure that the program established pursuant to this subparagraph includes the following:

(A) Cybersecurity incident reporting requirements that—

(i) extend beyond current mandatory incident reporting requirements;

(ii) set specific timeframes for all categories of incident reporting; and

(iii) creates a single clearinghouse for all mandatory incident reporting to the Department of Defense, including covered unclassified information, covered defense information, and classified information.

(B) A mechanism for developing a shared and real-time picture of the threat environment.

(C) Joint, collaborative, and co-located analytics.

(D) Investments in technology and capabilities to support automated detection and analysis across the defense industrial base.

(E) Coordinated intelligence sharing with relevant domestic law enforcement and counterintelligence agencies.

(F) A process for direct sharing of threat intelligence related to a specific defense industrial base entity with said entity.

(c) THREAT INTELLIGENCE PROGRAM PARTICIPATION.—

(1) PROHIBITION ON PROCUREMENT.—The Secretary of Defense may not procure or obtain, or extend or renew a contract to procure or obtain, any item, equipment, system, or service from any entity that is not a participant in the threat intelligence sharing program required by subsection (b).

(2) APPLICATION TO SUBCONTRACTORS.—No entity holding a Department of Defense contract may subcontract any portion of such contract to another entity unless that entity—

(A) meets the requirements of this section, and any rules promulgated pursuant thereto; or

(B) has received a waiver pursuant to subsection (e).

(3) IMPLEMENTATION.—In implementing the prohibition in paragraph (1), the Secretary of Defense—

(A) may create tiers of requirements and participation within the program based on—

(i) the role of and relative threats related to entities within the defense industrial base; and

(ii) cybersecurity maturity model certification level; and

(B) shall prioritize available funding and technical support to assist affected businesses, institutions, and organizations as is reasonably necessary for those affected entities to commence participation in the threat intelligence sharing program and to meet any applicable program requirements.

(d) EFFECTIVE DATES.—The prohibition under subsection (c)(1) shall take effect one year after the establishment of the threat intelligence sharing program required under subsection (b).

(e) WAIVER AUTHORITY.—

(1) WAIVER.— The Secretary of Defense may waive the prohibition in subsection (c)–

(A) with respect to an entity or class of entities, if the Secretary determines that the requirement to participate in a threat intelligence sharing program is unnecessary to protect the interests of the United States; or

(B) at the request of an entity, if the Secretary determines there is compelling justification for the waiver.

(2) PERIODIC REEVALUATION.—The Secretary of Defense shall periodically reevaluate any waiver issued pursuant to paragraph (1) and shall promptly revoke any waiver the Secretary determines is no longer warranted.

(f) EXISTING INFORMATION SHARING PROGRAMS.—The Secretary of Defense may utilize an existing Department of Defense information sharing program to satisfy the requirement in subsection (b) provided the existing program includes, or is modified to include, two-way sharing of threat information that is specifically relevant to the defense industrial base.

(g) REGULATIONS.—

(1) RULEMAKING AUTHORITY.—Not later than 180 days following the enactment of this Act, the Secretary of Defense shall promulgate such rules and regulations as are necessary to carry out this section.

(2) CMMC HARMONIZATION.—The Secretary of Defense shall ensure that the intelligence sharing requirements set forth in the rules and regulations promulgated pursuant to paragraph (1) consider an entity's maturity and role within the defense industrial base, consistent with the maturity certification levels established in the Department of Defense Cybersecurity Maturity Model Certification program.

(h) INTELLIGENCE QUERIES.—As part of the program established pursuant to subsection (b), the Secretary shall require defense industrial base entities holding a Department of Defense contract to consent to queries of foreign intelligence collection databases related to the entity as a condition of such contract.

## 6.2.2 Require Threat Hunting on DIB Networks

This proposal implements the Commission's recommendation to require threat hunting on defense industrial base (DIB) networks. This legislation will establish a program to seek and identify cybersecurity threats and vulnerabilities within the information systems of companies that make up the DIB. The Department of Defense (DoD) cannot procure items from entities that are not in compliance with the requirements of this threat identification program. However, the Secretary of Defense may waive the prohibition on procurement if he/she determines the requirement to participate in this program is unnecessary to protect the interests of the United States, or at the request of an entity that presents a compelling justification. The companies may also choose to use third-party hunt capabilities if certified by the DoD. These options should take into account variations in maturity across the DIB, drawing on the Cyber Maturity Model Certification (CMMC) regulation. When using the CMMC, it is important to note that level one through three are critical to also have a threat hunting capability established. Currently, only levels four and five have such a requirement.

---

**A BILL**

To establish a program to seek and identify cybersecurity threats and vulnerabilities within the information systems of companies that make up the defense innovation base of the United States, and for other purposes.

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

**SEC. 1. DEFENSE INDUSTRIAL BASE CYBERSECURITY THREAT HUNTING AND SENSING, DISCOVERY, AND MITIGATION.**

(a) DEFINITIONS.—In this section:

(1) DEFENSE INDUSTRIAL BASE.—The term "defense industrial base" means the worldwide industrial complex with capabilities to perform research and development, design, produce, deliver, and maintain military weapon systems, subsystems, components, or parts to meet military requirements.

(2) ADVANCED DEFENSE INDUSTRIAL BASE.—The term "advanced defense industrial base" means any defense industrial base entity holding a Department of Defense contract that requires a cybersecurity maturity model certification of level 4 or higher.

(b) DEFENSE INDUSTRIAL BASE CYBERSECURITY THREAT HUNTING.—

(1) IN GENERAL.—The Secretary of Defense shall establish a program to actively identify cybersecurity threats and vulnerabilities within the information

systems, including covered defense networks containing controlled unclassified information, of entities within the defense industrial base.

(2) PROGRAM LEVELS.—In establishing the program required by paragraph (1), the Secretary shall create a tiered program that takes into account—

(A) the cybersecurity maturity of the entity;

(B) the role of the entity within the defense industrial base;

(C) whether the entity possesses controlled unclassified information and covered defense networks; and

(D) the covered defense information an entity has access to as a result of contracts with the Department of Defense.

(3) PROGRAM REQUIREMENTS.—The program established pursuant to subsection (b) shall—

(A) include requirements for mitigating any vulnerabilities identified pursuant to the threat hunting program;

(B) provide a mechanism for the Department of Defense to share malicious code, indicators of compromise, and insights on the evolving threat landscape with entities in the defense industrial base;

(C) provide incentives for defense industrial base entities to share threat and vulnerability information collected pursuant to threat monitoring and hunt activities with the Department of Defense, including the National Security Agency's Cybersecurity Directorate; and

(D) mandate a minimum level of program participation for any entity that is part of the advanced defense industrial base.

(c) THREAT IDENTIFICATION PROGRAM PARTICIPATION.—

(1) PROHIBITION ON PROCUREMENT.—The Secretary of Defense may not procure or obtain, or extend or renew a contract to procure or obtain, any item, equipment, system, or service from any entity that is not in compliance with the requirements of the threat identification program required by subsection (b).

(2) IMPLEMENTATION.—In implementing the prohibition in paragraph (1), the Secretary of Defense shall prioritize available funding and technical support to assist affected businesses, institutions, and organizations as is reasonably

necessary for those affected entities to commence participation in the threat identification program and to meet any program requirements.

(d) EFFECTIVE DATES.—The prohibition pursuant to subsection (c)(1) shall take effect one year after the date of the enactment of this Act.

(e) WAIVER AUTHORITY.—

(1) WAIVER.—The Secretary of Defense may waive the prohibition in subsection (c)—

(A) with respect to an entity or class of entities, if the Secretary determines that the requirement to participate in a threat identification program is unnecessary to protect the interests of the United States; or

(B) at the request of an entity, if the Secretary determines there is a compelling justification for the waiver.

(2) PERIODIC REEVALUATION.—The Secretary of Defense shall periodically reevaluate any waiver issued pursuant to paragraph (1) and shall revoke any waiver the Secretary determines is no longer warranted.

(f) USE OF PERSONNEL AND THIRD-PARTY HUNT THREAT HUNTING AND SENSING CAPABILITIES.—In carrying out the program required by subsection (b), the Secretary of Defense may—

(1) utilize Department of Defense personnel to hunt for threats and vulnerabilities within the information systems of entities that contract with Department of Defense;

(2) certify third-party providers to hunt for threats and vulnerabilities on behalf of the Department of Defense;

(3) require the deployment of network sensing technologies capable of identifying and filtering malicious network traffic; or

(4) employ a combination of Department of Defense personnel and third-party providers and tools, as the Secretary determines necessary and appropriate for the defense industrial base entity.

(g) REGULATIONS.—

(1) RULEMAKING AUTHORITY.—Not later than 180 days following the enactment of this Act, the Secretary of Defense shall promulgate such rules and regulations as are necessary to carry out this section.

(2) CMMC HARMONIZATION.— In promulgating rules and regulations pursuant to paragraph (1), the Secretary of Defense shall consider how best to integrate the requirements of this section with the Department of Defense Cybersecurity Maturity Model Certification program.

## 6.2.4 Assess and Address Risks to NSS Posed by Quantum Computing

This proposal implements the Commission's recommendation to assess and address the risk to National Security Systems (NSSs) posed by quantum computing. As part of this process, the Secretary of Defense will complete a comprehensive assessment of the current and potential threats and risks posed by quantum computing to NSS.

---

**A BILL**

To require an assessment of the current and potential threats and risk posed by quantum computing to national security systems, and for other purposes.

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

**SEC. 1. ASSESSING RISK TO NATIONAL SECURITY OF QUANTUM COMPUTING.**

(a) REQUIREMENT FOR COMPREHENSIVE REVIEW.— To understand and prepare to counter the risks of quantum computing to national security, the Secretary of Defense shall, not later than December 31, 2021,—

(1) complete a comprehensive assessment of the current and potential threats and risks posed by quantum computing technologies to national security systems, including—

(A) identification of national security systems at risk;

(B) assessment of quantum resistant cryptographic standards and developmental timelines;

(C) feasibility of alternate quantum resistant models; and

(D) funding shortfalls in public and private developmental efforts; and

(2) make recommendations that prioritize, secure and resource the defense of national security systems identified in paragraph (1).

(b) STATUS ON PROGRESS.—The Secretary shall inform the congressional defense committees of the activities undertaken in the assessment conducted pursuant to this section as part of the quarterly cyber operations briefings required under section 484 of title 10, United States Code.

(c) REPORT.—

(1) the Secretary shall submit to the congressional defense committees a report on the assessment and recommendations developed pursuant to subsection (a); and

(2) the report under paragraph (1) may be submitted in unclassified form or classified form as necessary.

# 0.0 Extend the Cyberspace Solarium Commission to Track and Assess Implementation

This proposal implements the Commission's recommendation to extend a small element of the Commission from 120 days post report submission to 2 years post submission. This includes changes to Commissioner composition and staff composition and sizing, and it requires annual assessments be made to Congress in April 2021 and April 2022. This also calls for no more than $1,000,000 in additional funding. This is achieved by amending section 1652 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232).

---

**A BILL**

To extend the Cyberspace Solarium Commission to track and assess implementation of the Commission's recommendations, and for other purposes.

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

**SEC. 1. CYBERSPACE SOLARIUM COMMISSION.**

Section 1652 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232), is amended—

(a) in subsection (a)—

(1) in paragraph (1), by striking clauses (i) through (iv) in their entirety; and

(2) in paragraph (1)(B)(i), by striking "and who are appointed under clauses (iv) through (vii) of subparagraph (A)";

(b) in subsection (d)(2), by striking "Seven" and inserting "Six";

(c) in subsection (h)—

(1) in paragraph (1), by striking subparagraphs (B) and (C); and

(2) by striking paragraph (2);

(d) in subsection (i)(1)(B), by striking "officers or employees of the United States or";

(e) in subsection (k)—

(1) in paragraph (1), as amended by section 1626 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92; 133 Stat. 1198), by striking "September 1, 2019" and inserting "April 30, 2020";

(2) in paragraph (2)—

(A) in subparagraph (A), by striking "at the end of the 120-day period beginning on" and inserting "two years after";

(B) in subparagraph (B)—

(i) by striking "may use the 120-day" and inserting "shall use the two year";

(ii) by striking "concluding its activities, including providing testimony to Congress concerning the final report referred to in that paragraph and disseminating the report";

(C) by inserting a colon after "for the purposes of"; and

(D) by inserting the following new clauses after "purposes of:":

"(i) collecting and assessing comments and feedback from the Executive Branch Departments, academia, and the public on the analysis and recommendations contained in the Commission's report;

"(ii) collecting and assessing any developments in cybersecurity that may affect the recommendations in the Commission's report;

"(iii) reviewing the implementation of the recommendations contained in the Commission's report;

"(iv) revising, amending, or making new recommendations based on the assessments and reviews required by subparagraphs (i)-(iii);

"(v) providing an annual update to the Select Committee on Intelligence and the Committees on Armed Services, and Homeland Security and Governmental Affairs of the Senate; the Permanent Select Committee on Intelligence and the Committees on Armed Services and Homeland Security of the House of Representatives; and the Director of National Intelligence, the Secretary of Defense, and the Secretary of Homeland Security in a manner, format, determined by the Commission, any revisions,

amendments, or new recommendations reached by the Commission in subparagraph (iv);

"(iv) in subparagraph (B), by designating "concluding its activities, including providing testimony to Congress concerning the final report referred to in that paragraph and disseminating the report."; and

(3) In paragraph (2), by inserting after subparagraph (B) the following new subparagraph and clauses:

"(C) In the event that the Commission is extended, and the effective date of the extension comes after the time set for the Commission's termination, the Commission shall be deemed reconstituted with the same members and powers that existed at the time of termination of the Commission, except that—

"(i) a member of the Commission shall only serve if the member's position continues to be authorized under subsection (b);

"(ii) no compensation or entitlements relating to a person's status with the Commission shall be due for the period between the termination and reconstitution of the Commission;

"(iii) nothing in this paragraph shall be deemed as requiring the extension or reemployment of any staff member or contractor working for the Commission;

"(iv) the staff of the Commission shall be selected by the co-chairs of the Commission in accordance with paragraph (h)(1), shall be comprised of not more than four individuals, to include a staff director, will be resourced in accordance with paragraph (g)(4)(A) and, with the approval of the, co-chairs may be provided by contract with a non-governmental organization;

"(v) any unexpended funds made available for the use of the Commission shall continue to be available for use for the life of the Commission, as well as any additional funds appropriated to the Department of Defense that are made available to the Commission, provided that the total such funds do not exceed $1,000,000 from the reconstitution of the Commission to the completion of the Commission; and

"(vi) the requirement for an assessment of the final report in subsection (l) shall be required annually for a period of two years.".


U.S. CYBERSPACE SOLARIUM COMMISSION