AMENDMENT NO._____ Calendar No._____

Purpose: In the nature of a substitute.

IN THE SENATE OF THE UNITED STATES—117th Cong., 1st Sess.

S. 2491

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

Referred to the Committee on _____ and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT IN THE NATURE OF A SUBSTITUTE intended to be proposed by Ms. ROSEN (for herself and Ms. HASSAN)

Viz:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

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

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

SEC. 2. DEFINITIONS.

In this Act:

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

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

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

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

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

SEC. 101. INSTITUTE A 5-YEAR TERM FOR THE DIRECTOR OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

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

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

SEC. 102. PILOT PROGRAM ON CYBER THREAT INFORMATION COLLABORATION ENVIRONMENT.

(a) DEFINITIONS.—In this section:

(1) CRITICAL INFRASTRUCTURE INFORMATION.—The term ''critical infrastructure informa-

tion'' has the meaning given such term in section 2222 of the Homeland Security Act of 2002 (6 U.S.C. 671).

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

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

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

(5) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term ''information sharing and analysis organization'' has the meaning given such term in section 2222 of the Homeland Security Act of 2002 (6 U.S.C. 671).

(6) NON-FEDERAL ENTITY.—The term ''non-Federal entity'' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

(b) PILOT PROGRAM.—The Secretary, in consultation with the Secretary of Defense, the Director of National

Intelligence, the Director of the National Security Agency, and the Attorney General shall carry out a pilot program under which the Secretary shall develop an information collaboration environment and associated analytic tools that enable Federal and non-Federal entities to identify, mitigate, and prevent malicious cyber activity to—

(1) provide limited access to appropriate and operationally relevant data from unclassified and classified intelligence about cybersecurity risks and cybersecurity threats, as well as malware forensics and data from network sensor programs, on a platform that enables query and analysis;

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

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

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

(c) IMPLEMENTATION OF INFORMATION COLLABORATION ENVIRONMENT.—

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

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

(B) evaluate current programs, applications, or platforms intended to detect, identify, analyze, and monitor cybersecurity risks and cybersecurity threats;

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

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

(2) IMPLEMENTATION.—

(A) IN GENERAL.—Not later than 1 year after completing the evaluation required under paragraph (1)(B), the Secretary, acting through the Director of the Cybersecurity and Infrastructure Security Agency, and in consultation with the Secretary of Defense, the Director of National Intelligence, the Director of the National Security Agency, and the Attorney General, shall begin implementation of the environment to enable participants in the environment to develop and run analytic tools referred to in subsection (b) on specified data sets for the purpose of identifying, mitigating, and preventing malicious cyber activity that is a threat to public and private critical infrastructure.

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

(i) operate in a manner consistent with relevant privacy, civil rights, and civil liberties policies and protections, including such policies and protections established pursuant to section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485);

(ii) account for appropriate data standards and interoperability requirements, consistent with the standards set forth in subsection (d);

(iii) enable integration of current applications, platforms, data, and information, including classified information, in a manner that supports integration of unclassified and classified information on cybersecurity risks and cybersecurity threats;

(iv) incorporate tools to manage access to classified and unclassified data, as appropriate;

(v) ensure accessibility by entities the Secretary, in consultation with the Secretary of Defense, the Director of National Intelligence, the Director of the National Security Agency, and the Attorney General, determines appropriate;

(vi) allow for access by critical infrastructure stakeholders and other private sector partners, at the discretion of the Secretary, in consultation with the Secretary of Defense;

(vii) deploy analytic tools across classification levels to leverage all relevant data sets, as appropriate;

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

(ix) anticipate the integration of new technologies and data streams, including data from government-sponsored network sensors or network-monitoring programs deployed in support of non-Federal entities.

(3) ANNUAL REPORT REQUIREMENT ON THE IMPLEMENTATION, EXECUTION, AND EFFECTIVENESS OF THE PILOT PROGRAM.—Not later than 1 year after the date of enactment of this Act, and every year thereafter until the date that is 1 year after the pilot program under this section terminates under subsection (e), the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, and the Select Committee on Intelligence of the Senate and the Committee on Homeland Security, the Committee on the Judiciary, and the Permanent Select

Committee on Intelligence of the House of Representatives a report that details—

(A) Federal Government participation in the environment, including the Federal entities participating in the environment and the volume of information shared by Federal entities into the environment;

(B) non-Federal entities' participation in the environment, including the non-Federal entities participating in the environment and the volume of information shared by non-Federal entities into the environment;

(C) the impact of the environment on positive security outcomes in the Federal Government and non-Federal entities;

(D) barriers identified to fully realizing the benefit of the environment both for the Federal Government and non-Federal entities; and

(E) additional authorities or resources necessary to successfully execute the environment.

(d) CYBER THREAT DATA STANDARDS AND INTEROPERABILITY.—

(1) ESTABLISHMENT.—The Secretary, in coordination with the Secretary of Defense, the Director of National Intelligence, the Director of the Na-

tional Security Agency, and the Attorney General, shall establish data standards and requirements for non-Federal entities to participate in the environment.

(2) DATA STREAMS.—The Secretary shall identify, designate, and periodically update programs that shall participate in or be interoperable with the environment, which may include—

(A) network-monitoring and intrusion detection programs;

(B) cyber threat indicator sharing programs;

(C) certain government-sponsored network sensors or network-monitoring programs;

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

(E) malware forensics and reverse-engineering programs.

(3) DATA GOVERNANCE.—The Secretary, in consultation with the Secretary of Defense, the Director of National Intelligence, the Director of the National Security Agency, and the Attorney General 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 public and private sector critical infrastructure entities that apply to critical infrastructure information.

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

(e) DURATION.—The pilot program under this section shall terminate on the date that is 5 years after the date of enactment of this Act.

TITLE II—IMPROVING SECURITY IN THE NATIONAL CYBER ECOSYSTEM

SEC. 201. REPORT ON CYBERSECURITY CERTIFICATIONS AND LABELING.

Not later than October 1, 2022, the National Cyber Director, in consultation with the Director of the National Institute of Standards and Technology and 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 a report that—

(1) identifies and assesses existing efforts by the Federal Government to create, administer, or

otherwise support the use of certifications or labels to communicate the security or security characteristics of information technology or operational technology products and services; and

(2) assesses the viability of and need for a new program at the Department to harmonize information technology and operational technology product and service security certification and labeling efforts across the Federal Government and between the Federal Government and the private sector.

SEC. 202. SECURE FOUNDATIONAL INTERNET PROTOCOLS.

(a) DEFINITIONS.—In this section:

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

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

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

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

(1) PROTOCOL SECURITY STRATEGY.—In order to encourage implementation of measures to secure foundational internet protocols by information and communications technology infrastructure providers, not later than 180 days after the date of enactment of this Act, the Assistant Secretary for Communications and Information of the Department of Commerce, in coordination with the Director of the National Institute Standards and Technology and the Director of the Cybersecurity and Infrastructure Security Agency, shall establish a working group composed of appropriate stakeholders, including representatives of the Internet Engineering Task Force and information and communications technology infrastructure providers, to prepare and submit to Congress a strategy to encourage implementation of measures to secure the border gateway protocol and the domain name system.

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

(A) articulate the motivation and goal of the strategy to reduce incidents of border gateway protocol hijacking and domain name system hijacking;

(B) articulate the security and privacy benefits of implementing the most up-to-date and secure instances of the border gateway protocol and the domain name system and the burdens of implementation and the entities on whom those burdens will most likely fall;

(C) identify key United States and international stakeholders;

(D) outline varying measures that could be used to implement security or provide authentication for the border gateway protocol and the domain name system;

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

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

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

TITLE III—ENABLING THE NATIONAL CYBER DIRECTOR

SEC. 301. ESTABLISHMENT OF HIRING AUTHORITIES FOR THE OFFICE OF THE NATIONAL CYBER DIRECTOR.

(a) DEFINITIONS.—In this section—

(1) the term ''Director'' means the National Cyber Director;

(2) the term ''excepted service'' has the meaning given such term in section 2103 of title 5, United States Code;

(3) the term ''Office'' means the Office of the National Cyber Director;

(4) the term ''qualified position'' means a position identified by the Director under subsection (b)(1)(A), in which the individual occupying such position performs, manages, or supervises functions that execute the responsibilities of the Office.

(b) HIRING PLAN.—The Director shall, for purposes of carrying out the functions of the Office—

(1) craft an implementation plan for positions in the excepted service in the Office, which shall propose—

(A) qualified positions in the Office, as the Director determines necessary to carry out the responsibilities of the Office; and

(B) subject to the requirements of paragraph (2), rates of compensation for an individual serving in a qualified position;

(2) propose rates of basic pay for qualified positions, which shall—

(A) be determined in relation to the rates of pay provided for employees in comparable positions in the Office, in which the employee occupying the comparable position performs, manages, or supervises functions that execute the mission of the Office; and

(B) subject to the same limitations on maximum rates of pay and consistent with section 5341 of title 5, United States Code, adopt such provisions of that title to provide for prevailing rate systems of basic pay and apply those provisions to qualified positions for em-

ployees in or under which the Office may employ individuals described by section 5342(a)(2)(A) of such title; and

(3) craft proposals to provide—

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

(B) employees in a qualified position for which the Director proposes a rate of basic pay under paragraph (2) an allowance under section 5941 of title 5, United States Code, on the same basis and to the same extent as if the employee was an employee covered by such section, including eligibility conditions, allowance rates, and all other terms and conditions in law or regulation.