Calendar No. 670

117TH CONGRESS *2d Session*	SENATE	REPORT 117–271

DEFENSE OF UNITED STATES INFRASTRUCTURE ACT OF 2021

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

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

DECEMBER 19, 2022.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE

39–010 WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
ALEX PADILLA, California
JON OSSOFF, Georgia

ROB PORTMAN, Ohio
RON JOHNSON, Wisconsin
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
JEFFREY D. ROTHBLUM, *Senior Professional Staff Member*
PAMELA THIESSEN, *Minority Staff Director*
SAM J. MULOPULOS, *Minority Deputy Staff Director*
WILLIAM H.W. MCKENNA, *Minority Chief Counsel*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 670

117TH CONGRESS *2d Session* | SENATE | REPORT 117–271

DEFENSE OF UNITED STATES INFRASTRUCTURE ACT OF 2021

DECEMBER 19, 2022.—Ordered to be printed

Mr. PETERS, from the Committee on Homeland Security and Governmental Affairs, submitted the following

R E P O R T

[To accompany S. 2491]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (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, having considered the same, reports favorably thereon with an amendment, in the nature of a substitute and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

S. 2491, the *Defense of United States Infrastructure Act of 2021*, would amend the Homeland Security Act of 2002 to strengthen the authorities of government cybersecurity officials, improve information sharing, and enhance the security of software and internet

protocols. S. 2491 is based on the recommendations of the U.S. Cyberspace Solarium Commission (the Commission)—a congressionally mandated commission comprised of legislators, federal officials, and private sector stakeholders. The Commission's work included interviewing numerous cybersecurity experts in academia, nonprofit, industry, and government sectors, and its report offered over 50 legislative recommendations to improve the U.S. cybersecurity posture. S. 2491 includes a number of the Commission's recommendations.[1]

II. Background and Need for the Legislation

The Commission identified a need to bolster federal cybersecurity leaders' positions in order to improve the government's ability to respond to cybersecurity threats against both the government and private sector entities. One such recommendation was to strengthen the Director of the Cybersecurity and Infrastructure Security Agency (CISA) by setting a fixed term limit for the role. The Director of CISA is currently a Senate confirmed political appointee without a specific term limit, like most other political appointees.[2] The Commission recommended that the Director be given a five-year term limit, which would be half of the length of the Federal Bureau of Investigation (FBI) Director's term of 10 years and the same term length of the Transportation Security Agency (TSA) Administrator.[3] This would allow greater continuity and empower the Director to develop and implement multi-year strategies for CISA.[4]

The Commission also recommended that Congress create the National Cyber Director (NCD) to be the President's primary cybersecurity advisor, and Congress established the position in the National Defense Authorization Act for Fiscal Year 2021.[5] However, the NCD is currently unable to offer excepted services positions, which may hinder the NCD's ability to hire and retain staff who are offered competitive compensation to the private sector. This legislation would require the NCD create an implementation plan to hire excepted service employees.

The Commission found barriers to sharing cyber threat intelligence among agencies and with private sector partners. While the federal government has a number of programs that collect information on cybersecurity threats, "the data or information is not routinely shared or cross-correlated at the speed and scale necessary for rapid detection and identification."[6] Without data that can be queried and analyzed in real-time, the federal government has a fragmented picture of the threat landscape, which can cause "confusion" and add "burdens" to the private sector, limiting the effectiveness of the government and private sector to respond to cyber threats.[7]

---

[1] United States Cyberspace Solarium Commission, *Final Report* (Mar. 2020) (https://www.solarium.gov/report).
[2] Homeland Security Act of 2002, as amended, Pub. L. 107–296, Sec. 103.
[3] Pub. L. No. 94–503 (1976) and 49 U.S.C. § 114.
[4] United States Cyberspace Solarium Commission, *Final Report* (Mar. 2020) (https://www.solarium.gov/report).
[5] Pub. L. No. 116–283 (2021).
[6] United States Cyberspace Solarium Commission, *Final Report* (Mar. 2020) (https://www.solarium.gov/report).
[7] *Id*.

Additionally, the Commission's report discussed the need to improve the "cyber ecosystem," including improving the security of Border Gateway Protocol (BGP) and the Domain Name System (DNS), key components of the internet which have been exploited by malicious actors.[8] BGP was not designed to be secure and is vulnerable to cyber-attacks; the National Institute of Standards and Technology (NIST) found that the exploitation of such vulnerabilities could have far-reaching effects. NIST Special Publication 800–54, *Border Gateway Protocol Security*, states that "[b]ecause of the volume of commercial transactions conducted over the Internet, plus increasing use of the Internet for voice communications (voice over IP [VOIP]), such an outage could have a significant impact on the economy, and possibly interrupt critical functions such as emergency services communications."[9] One report found that in the first five months of 2020, 23% of all incidents affecting the functionality of the BGP were caused by cyber attacks.[10]

DNS is the system by which a domain name is translated into an Internet Protocol (IP) address, thereby directing the end-user to the appropriate source without the user having to know the series of numbers contained in the IP address.[11] Because DNS was not designed to be secure, attackers have been able to exploit characteristics of the system to "to direct users to fake websites designed to steal login credentials and other sensitive information."[12] The legislation would require the Department of Commerce to consult with relevant federal agencies and private-sector stakeholders to develop a strategy to better secure BGP and DNS.

Cybersecurity experts and the Commission have called for a "cyber energy green star" or "cyber nutrition label" to inform consumers and businesses of the software that is contained in their applications or devices.[13] S. 2491 would require the NCD to provide a report to Congress on current federal efforts to develop such security certifications and labels for information technology and operational technology products and services.

---

[8] There have been numerous instances of cybersecurity attacks on both BGP and DNS by malicious actors. *E.g., Russian telco hijacks internet traffic for Google, AWS, Cloudflare, and others*, ZDNET (Apr. 5, 2020) (https://www.zdnet.com/article/russian-telco-hijacks-internet-traffic-for-google-aws-cloudflare-and-others) and Mandiant, *Global DNS Hijacking Campaign: DNS Record Manipulation at Scale* (Jan. 9, 2019) (https://www.mandiant.com/resources/blog/global-dns-hijacking-campaign-dns-record-manipulation-at-scale)

[9] National Institute of Standards and Technology, *Border Gateway Protocol Security*, (NIST Special Publication 800–54), at 3–1 (https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800–54.pdf).

[10] Atlantic Council, *The Politics of Internet Security: Private Industry and the Future of the Web*, (Oct. 5, 2020); (https://www.atlanticcouncil.org/in-depth-research-reports/report/the-politics-of-internet-security-private-industry-and-the-future-of-the-web/#routing).

[11] National Institute of Standards and Technology, *Secure Domain Name System (DNS) Deployment Guide*, (NIST Special Publication 800–81–2) (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800–81–2.pdf).

[12] Cloudflare, *The global DNS hijacking threat* (https://www.cloudflare.com/learning/security/global-dns-hijacking-threat) (accessed Dec. 6, 2022).

[13] United States Cyberspace Solarium Commission, *Final Report* (Mar. 2020) (https://www.solarium.gov/report); Public Knowledge, *Creating a Cybersecurity "Energy Star,"* (Jul. 20, 2018) https://publicknowledge.org/creating-a-cybersecurity-energy-star/; Symantec Enterprise Blogs, *Why we need a Security and Privacy "Nutrition Label" for IoT Devices*, (Feb. 19 2019) (https://symantec-enterprise-blogs.security.com/blogs/expert-perspectives/why-we-need-security-and-privacy-nutrition-label-iot-devices).

III. LEGISLATIVE HISTORY

Senators King (I–ME), Rounds (R–SD), and Sasse (R–NE) introduced S. 2491, the Defense of United States Infrastructure Act of 2021, on July 27, 2021. The bill was referred to the Senate Committee on Homeland Security and Governmental Affairs. Senator Rosen (D–NV) joined as a cosponsor on August 3, 2021; Senator Hassan (D–NH) joined as a cosponsor on October 19, 2021; and Senator Ossoff (D–GA) joined as a cosponsor on November 4, 2021.

The Committee considered S. 2491 at a business meeting on November 3, 2021. During the business meeting, Senators Rosen and Hassan offered a substitute amendment to make technical amendments and strike several sections of the introduced bill, which was adopted by unanimous consent. The Committee ordered the bill, as amended, reported favorably by voice vote with Senators Johnson, Scott, and Hawley recorded as voting "no." Senators present for the vote were: Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Johnson, Lankford, Romney, Scott, and Hawley.

IV. SECTION-BY-SECTION ANALYSIS OF THE BILL, AS REPORTED

Section 1. Short title

This section designates the short title of the bill as the "Defense of United States Infrastructure Act of 2021" and lists a table of contents.

Section 2. Definitions

This section defines "critical infrastructure," "cybersecurity risk," "Department," and "Secretary."

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

Section 101. Institute a 5-year term for the Director of the Cybersecurity and Infrastructure Security Agency

Subsection (a) amends the Homeland Security Act of 2002 to create a five-year term for the Director of CISA.

Subsection (b) creates a transition rule such that the five-year term will take effect on the first appointment of the CISA Director made on or after the date of enactment of this Act.

Section 102. Pilot program on cyber threat information collaboration environment

Subsection (a) defines "critical infrastructure information," "cyber threat indicator," "cybersecurity threat," "environment," "information sharing and analysis organization," and "non-federal entity."

Subsection (b) requires the Secretary of the Department of Homeland Security (DHS), in consultation with the Secretary of Defense, the Director of National Intelligence, the Director of the National Security Agency, and the Attorney General to create a pilot program to develop an information collaboration environment and associated analytic tools that enable federal and non-federal entities to identify, mitigate, and prevent malicious cyber activity.

Subsection (c) requires the Secretary of DHS to coordinate with Secretary of Defense, the Director of National Intelligence, the Director of the National Security Agency, and the Attorney General

to identify, inventory, and evaluate existing federal sources of classified and unclassified information; evaluate current programs, applications, or platforms intended to detect, identify, analyze, and monitor cybersecurity risks and cybersecurity threats; consult with public and private sector critical infrastructure entities to identify public and private critical infrastructure cyber threat capabilities, needs, and gaps; and identify existing tools, capabilities, and systems that may be adapted to achieve the purposes of the environment to maximize return on investment and minimize cost. This subsection also requires the Secretary of DHS to begin implementing the environment no later than one year after completing the evaluation. This subsection provides requirements that the environment must abide by. No later than a year after the enactment of this bill and every year thereafter until the date that is one year after the pilot program terminates, the Secretary of DHS shall submit to Congress a report on federal government participation in the environment; non-federal entity participation in the environment; the impact on positive security outcomes; barriers to fully realizing the benefit of the environment; and any additional authorities or resources to execute the environment.

Subsection (d) requires the Secretary of DHS to coordinate with Secretary of Defense, the Director of National Intelligence, the Director of the National Security Agency, and the Attorney General to establish data standards and requirements for non-Federal entities to participate in the environment.

Subsection (e) requires the pilot to sunset after five years after the date of the enactment of this Act.

TITLE II—IMPROVING SECURITY IN THE NATIONAL CYBER ECOSYSTEM

Section 201. Report on cybersecurity certifications and labeling

This section requires the NCD, in consultation with the Director of the NIST and the Director of CISA to identify 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 assesses the viability of and need for a new program at DHS 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.

Section 202. Secure foundational internet protocols

Subsection (a) defines "border gateway protocol," "domain name system," and "information and communications technology infrastructure providers."

Subsection (b) requires the Assistant Secretary for Communications and Information of the Department of Commerce, in coordination with the Director of NIST and the Director of CISA to establish a working group of appropriate stakeholders to submit to Congress a strategy to encourage implementation of measures to secure the border gateway protocol and the domain name system.

TITLE III—ENABLING THE NATIONAL CYBER DIRECTOR

Section 301. Establishment of hiring authorities for the Office of the National Cyber Director

Subsection (a) defines "director," "excepted service," "office," and "qualified position."

Subsection (b) requires the NCD to craft an implementation plan for positions in the excepted service in the Office of the NCD, propose rates of basic pay for qualified positions, and detail proposals to provide employees in qualified positions compensation.

V. Evaluation of Regulatory Impact

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

VI. Congressional Budget Office Cost Estimate

U.S. Congress,
Congressional Budget Office,
Washington, DC, January 11, 2022.

Hon. Gary C. Peters,
Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has prepared the enclosed cost estimate for S. 2491, the Defense of United States Infrastructure Act of 2021.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Aldo Prosperi.

Sincerely,

Phillip L. Swagel,
Director.

Enclosure.

S. 2491, Defense of United States Infrastructure Act of 2021

As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on November 3, 2021

By Fiscal Year, Millions of Dollars	2022	2022-2026	2022-2031
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	*	16	not estimated

Statutory pay-as-you-go procedures apply?	No	Mandate Effects	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2032?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

* = between zero and $500,000.

S. 2491 would require the Department of Homeland Security (DHS) to carry out a five-year program to share information about cybersecurity threats and vulnerabilities with the owners of critical infrastructure (such as power generation and water treatment plants). The bill also would require DHS to report on other federal cybersecurity efforts, such as providing safety labels for cybersecurity products and mitigating malicious Internet traffic.

Using information from other agencies that share information about cyber threats—including the Department of Defense and the Office of the Director of National Intelligence—CBO anticipates that DHS would need ten full-time employees to create and manage the pilot program required under S. 2491. For this estimate, CBO assumes that the bill will be enacted in fiscal year 2022 and that DHS would begin to operate the pilot program in 2023. CBO estimates that staff salaries and software development costs to share cyber alerts would cost $4 million annually and total $16 million over the 2022–2026 period; such spending would be subject to the availability of appropriated funds.

The CBO staff contact for this estimate is Aldo Prosperi. The estimate was reviewed by Leo Lex, Deputy Director of Budget Analysis.

VII. Changes in Existing Law Made by the Bill, as Reported

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows: (existing law proposed to be omitted is enclosed in brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

UNITED STATES CODE

* * * * * * *

TITLE 6—DOMESTIC SECURITY

* * * * * * *

CHAPTER 1—HOMELAND SECURITY ORGANIZATION

* * * * * * *

Subchapter XVIII—Cybersecurity and Infrastructure Security Agency

PART A—CYBERSECURITY AND INFRASTRUCTURE SECURITY

* * * * * * *

SEC. 652. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

(a) * * *

(b) DIRECTOR.—

(1) IN GENERAL.—The Agency shall be headed by a Director of Cybersecurity and Infrastructure Security (in this part referred to as the "Director"), who shall report to the Secretary. *The term of office of an individual serving as Director shall be 5 years.*

* * * * * * *

○