116TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
116–193

CYBERSECURITY VULNERABILITY REMEDIATION ACT

AUGUST 30, 2019.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. THOMPSON of Mississippi, from the Committee on Homeland Security, submitted the following

R E P O R T

[To accompany H.R. 3710]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 3710) to amend the Homeland Security Act of 2002 to provide for the remediation of cybersecurity vulnerabilities, and for other purposes, having considered the same, report favorably thereon without amendment and recommend that the bill do pass.

CONTENTS

PURPOSE AND SUMMARY

H.R. 3710, the "Cybersecurity Vulnerability Remediation Act," seeks to improve how the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) helps Federal and non-Federal entities manage known cybersecu-

rity risks. Toward that end, the bill would authorize the CISA Director to identify, develop, and disseminate actionable protocols to mitigate cybersecurity vulnerabilities—including for software or hardware that is no longer supported by the vendor. Additionally, the bill would authorize the DHS Under Secretary for Science and Technology to establish an incentive-based program that allows industry, individuals, academia, and others to compete in providing remediation solutions for cybersecurity vulnerabilities.

BACKGROUND AND NEED FOR LEGISLATION

The Cybersecurity and Infrastructure Security Agency (CISA) is responsible for Federal network protection and providing voluntary cybersecurity services to non-Federal entities. Toward that end, CISA has invested in developing systems to catalogue cybersecurity vulnerabilities. Leveraging the Common Vulnerabilities and Exposures (CVE) database and in partnership with the National Institute of Standard and Technology (NIST), CISA established the National Vulnerability Database (NVD) to assess the severity of cybersecurity vulnerabilities.

Even with these this tools, however, owners and operators of public and private information systems are not consistently able to manage known security risks and combat cyber threats. H.R. 3710 would authorize CISA to develop and distribute "playbooks," in consultation with private sector experts, to provide procedures and mitigation strategies for the most critical, known vulnerabilities—especially those affecting software or hardware that is no longer supported by a vendor. The playbooks would be available to Federal agencies, industry, and other stakeholders. H.R. 3710 would also allow for the DHS Science and Technology Directorate (S&T), in consultation with CISA, to establish a competition program for industry, individuals, academia, and others to provide remediation solutions for cybersecurity vulnerabilities that are no longer supported.

HEARINGS

For the purpose of section 103(i) of H. Res. 6 of the 116th Congress the following related hearings were held:

A Full Committee hearing entitled "Defending Our Democracy: Building Partnerships to Protect America's Elections," on February 13, 2019 and a June 25, 2019, a hearing held by the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation entitled "Cybersecurity Challenges for State and Local Governments: Assessing How the Federal Government Can Help."

COMMITTEE CONSIDERATION

The Committee met on July 17, 2019, with a quorum being present, to consider H.R. 3710 and ordered the measure to be reported to the House with a favorable recommendation, without amendment, by unanimous consent.

COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

CONGRESSIONAL BUDGET OFFICE ESTIMATE NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

With respect to the requirements of clause 3(c)(2) of rule XIII of the Rules of the House of Representatives and section 308(a) of the Congressional Budget Act of 1974 and with respect to requirements of clause (3)(c)(3) of rule XIII of the Rules of the House of Representatives and section 402 of the Congressional Budget Act of 1974, The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, August 1, 2019.

Hon. BENNIE G. THOMPSON,
Chairman, Committee on Homeland Security,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 3710, the Cybersecurity Vulnerability Remediation Act.

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.

H.R. 3710, Cybersecurity Vulnerability Remediation Act
As ordered reported by the House Committee on Homeland Security on July 17, 2019

By Fiscal Year, Millions of Dollars	2019	2019-2024	2019-2029
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	0	44	not estimated

		Mandate Effects	
Statutory pay-as-you-go procedures apply?	No	Contains intergovernmental mandate?	No
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2030?	No	Contains private-sector mandate?	No

H.R. 3710 would authorize the Department of Homeland Security (DHS) to disseminate information to the public about vulnerabilities in the software and hardware of information systems. The bill also would authorize DHS to establish an award program to encourage independent researchers to identify and report vulnerabilities and solutions for those vulnerabilities to the department.

DHS is already performing many of the cybersecurity activities that would be authorized by H.R. 3710. The department manages several programs that provide services and information to help system administrators, software manufacturers, and the general public identify cyber vulnerabilities. For example, the DHS Common Vulnerabilities and Exposures program helps software vendors identify risks and communicate to their customers how vulnerabilities affect their products and services.

To estimate the cost of providing incentive payments to independent researchers, CBO used information about similar programs of other federal agencies. For example, the General Services Administration (GSA) offers payments to individual researchers through its Bug Bounty program for each vulnerability identified. Those payments range from $150 to $5,000 based on how critical the potential target is to GSA's operations. On the basis of budget data from those related programs, CBO estimates that making incentive payments to independent researchers for identifying vulnerabilities would cost $11 million each year. CBO expects that DHS would be ready to implement the program beginning in 2021. Thus, CBO estimates that enacting H.R. 3710 would cost $44 million over the 2019–2024 period. Such spending would be subject to availability of appropriated funds.

Areas of uncertainty in that estimate include expectations about the criteria DHS would use in awarding payments to independent researchers. H.R. 3710 would give DHS broad latitude in establishing the criteria under which it would provide cash payments. CBO assumes that the department would limit payments to actions that protect government systems. The budgetary effects of the bill would be significantly larger than this estimate if DHS also provides payments for actions that protect nonfederal systems.

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

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 3710 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

PERFORMANCE GOALS AND OBJECTIVES

The Committee states that pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, H.R. 3710 would authorize the CISA Director to identify, develop, and share mitigation protocols for managing security vulnerabilities and addressing cybersecurity risk. Additionally the bill would authorize the DHS Under Secretary for Science and Technology to establish an incentive-based program that allows industry, individuals, academia, and others to compete in providing remediation solutions for cybersecurity vulnerabilities.

ADVISORY ON EARMARKS

In compliance with rule XXI of the Rules of the House of Representatives, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(d), 9(e), or 9(f) of the rule XXI.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

This section provides that the bill may be cited as the "Cybersecurity Vulnerability Remediation Act".

Sec 2. Cybersecurity vulnerabilities

This section provides that the term "cybersecurity vulnerability" has the meaning given the term "security vulnerability" in section 102 of the Cybersecurity Information Sharing Act of 2015.

The section authorizes the CISA Director to, as appropriate, identify, develop, and disseminate actionable protocols to mitigate cybersecurity vulnerabilities, including in circumstances in which such vulnerabilities exist because software or hardware is no longer supported by a vendor. The section further provides that the National Cybersecurity and Communications Integration Center shall share mitigation protocols to counter cybersecurity vulnerabilities.

Sec 3. Report on cybersecurity vulnerabilities

This section provides that not later than one year after the date of the enactment of this Act, the CISA Director shall submit to the Committee on Homeland Security of the House of Representatives

and the Committee on Homeland Security and Governmental Affairs of the Senate a report on how the Agency carries out subsection (m) of section 2209 of the Homeland Security Act of 2002 to coordinate vulnerability disclosures, including disclosures of cybersecurity vulnerabilities (as such term is defined in such section), and subsection (n) of such section (as added by section 2) to disseminate actionable protocols to mitigate cybersecurity vulnerabilities, that includes the following: a description of the policies and procedures relating to the coordination of vulnerability disclosures; a description of the levels of activity in furtherance of such subsections (m) and (n) of such section 2209; any plans to make further improvements to how information provided pursuant to such subsections can be shared (as such term is defined in such section 2209) between the Department and industry and other stakeholders; any available information on the degree to which such information was acted upon by industry and other stakeholders; a description of how privacy and civil liberties are preserved in the collection, retention, use, and sharing of vulnerability disclosures.

Sec 4. Competition relating to cybersecurity vulnerabilities

This section authorizes the Under Secretary for Science and Technology at the Department of Homeland Security, consultation with the CISA Director, to establish an incentive-based program that allows industry, individuals, academia, and others to compete in providing remediation solutions for cybersecurity vulnerabilities (as such term is defined in section 2209 of the Homeland Security Act of 2002, as amended by section 2). The Committee believes that the establishment of an incentives-based program could enhance CISA's ability to develop timely playbooks to mitigate known cybersecurity vulnerabilities that could be exploited.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

* * * * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Subtitle A—Cybersecurity and Infrastructure Security

* * * * * * *

SEC. 2209. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

(a) DEFINITIONS.—In this section—

(1) the term "cybersecurity risk"—

(A) means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism; and

(B) does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement;

(2) the terms "cyber threat indicator" and "defensive measure" have the meanings given those terms in section 102 of the Cybersecurity Act of 2015;

(3) the term "incident" means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system;

(4) the term "information sharing and analysis organization" has the meaning given that term in section 2222(5);

(5) the term "information system" has the meaning given that term in section 3502(8) of title 44, United States Code; [and]

(6) the term "cybersecurity vulnerability" has the meaning given the term "security vulnerability" in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501); and

[(6)] *(7)* the term "sharing" (including all conjugations thereof) means providing, receiving, and disseminating (including all conjugations of each of such terms).

(b) CENTER.—There is in the Department a national cybersecurity and communications integration center (referred to in this section as the "Center") to carry out certain responsibilities of the Director. The Center shall be located in theCybersecurity and Infrastructure Security Agency.The head of the Center shall report to the AssistantDirector for Cybersecurity.

(c) FUNCTIONS.—The cybersecurity functions of the Center shall include—

(1) being a Federal civilian interface for the multi-directional and cross-sector sharing of information related to cyber threat indicators, defensivemeasures, cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities, including the implementationof title I of the Cybersecurity Act of 2015;

(2) providing shared situational awareness to enable real-time, integrated, and operational actions across the Federal Government and non-Federal entities to address cybersecurity risks and incidents to Federal and non-Federal entities;

(3) coordinating the sharing of information related to cyber threat indicators, defensive measures,cybersecurity risks, and incidents across the Federal Government;

(4) facilitating cross-sector coordination to address cybersecurity risks and incidents, including cybersecurity risks and incidents that may be related or could have consequential impacts across multiple sectors;

(5)(A) conducting integration and analysis, including cross-sector integration and analysis, of cyber threat indicators, defensivemeasures, cybersecurity risks, and incidents; [and]

(B) sharing mitigation protocols to counter cybersecurity vulnerabilities pursuant to subsection (n); and

[(B)] *(C)* sharing the analysis conducted under subparagraph (A) *and mitigation protocols to counter cybersecurity vulnerabilities in accordance with subparagraph (B)* with Federal and non-Federal entities;

(6) upon request, providing timely technical assistance, risk management support, and incident response capabilities to Federal and non-Federal entities with respect to cyber threat indicators, defensive measures, cybersecurityrisks, and incidents, which may include attribution, mitigation, and remediation;

(7) providing information and recommendations on security and resilience measures to Federal and non-Federal entities, including information and recommendations to—

(A) facilitate information security;

(B) strengthen information systems against cybersecurity risks and incidents; and

(C) [sharing] *share* cyber threat indicators and defensive measures;

(8) engaging with international partners, in consultation with other appropriate agencies, to—

(A) collaborate on cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents; and

(B) enhance the security and resilience of global cybersecurity;

(9) sharing cyber threat indicators, defensive measures, *mitigation protocols to counter cybersecurity vulnerabilities,* and other information related to cybersecurity risks and incidents with Federal and non-Federal entities, including across sectors of critical infrastructure and with State and major urban area fusion centers, as appropriate;

(10) participating, as appropriate, in national exercises run by the Department; and

(11) in coordination with the Emergency Communications Division of the Department, assessing and evaluating consequence, vulnerability, and threat information regarding cyber incidents to public safety communications to help facilitate continuous improvements to the security and resiliency of such communications.

(d) COMPOSITION.—

(1) IN GENERAL.—The Center shall be composed of—

(A) appropriate representatives of Federal entities, such as—

(i) sector-specific agencies;

(ii) civilian and law enforcement agencies; and

(iii) elements of the intelligence community, as that term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4));

(B) appropriate representatives of non-Federal entities, such as—

(i) State, local, and tribal governments;

(ii) information sharing and analysis organizations, including information sharing and analysis centers;

(iii) owners and operators of critical information systems; and

(iv) private entities;

(C) components within the Center that carry out cybersecurity and communications activities;

(D) a designated Federal official for operational coordination with and across each sector;

(E) an entity that collaborates with State and local governments on cybersecurity risks and incidents, and has entered into a voluntary information sharing relationship with the Center; and

(F) other appropriate representatives or entities, as determined by the Secretary.

(2) INCIDENTS.—In the event of an incident, during exigent circumstances the Secretary may grant a Federal or non-Federal entity immediate temporary access to the Center.

(e) PRINCIPLES.—In carrying out the functions under subsection (c), the Center shall ensure—

(1) to the extent practicable, that—

(A) timely, actionable, and relevant cyber threat indicators, defensive measures, and information related to cybersecurity risks, incidents, and analysis is shared;

(B) when appropriate, cyber threat indicators, defensive measures, and information related to cybersecurity risks, incidents, and analysis is integrated with other relevant information and tailored to the specific characteristics of a sector;

(C) activities are prioritized and conducted based on the level of risk;

(D) industry sector-specific, academic, and national laboratory expertise is sought and receives appropriate consideration;

(E) continuous, collaborative, and inclusive coordination occurs—

(i) across sectors; and

(ii) with—

(I) sector coordinating councils;

(II) information sharing and analysis organizations; and

(III) other appropriate non-Federal partners;

(F) as appropriate, the Center works to develop and use mechanisms for sharing information related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents that are technology-neutral, interoperable, real-time, cost-effective, and resilient;

(G) the Center works with other agencies to reduce unnecessarily duplicative sharing of information related to

cyber threat indicators, defensive measures, cybersecurity risks, and incidents; and[;]

(H) the Center designates an agency contact for non-Federal entities;

(2) that information related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents is appropriately safeguarded against unauthorized access or disclosure; and

(3) that activities conducted by the Center comply with all policies, regulations, and laws that protect the privacy and civil liberties of United States persons, including by working with the Privacy Officer appointed under section 222 to ensure that the Center follows the policies and procedures specified in subsections (b) and (d)(5)(C) of section 105 of the Cybersecurity Act of 2015.

(f) NO RIGHT OR BENEFIT.—

(1) IN GENERAL.—The provision of assistance or information to, and inclusion in the Center of, governmental or private entities under this section shall be at the sole and unreviewable discretion of the Director.

(2) CERTAIN ASSISTANCE OR INFORMATION.—The provision of certain assistance or information to, or inclusion in the Center of, one governmental or private entity pursuant to this section shall not create a right or benefit, substantive or procedural, to similar assistance or information for any other governmental or private entity.

(g) AUTOMATED INFORMATION SHARING.—

(1) IN GENERAL.—The Director, in coordination with industry and other stakeholders, shall develop capabilities making use of existing information technology industry standards and best practices, as appropriate, that support and rapidly advance the development, adoption, and implementation of automated mechanisms for the sharing of cyber threat indicators and defensive measures in accordance with title I of the Cybersecurity Act of 2015.

(2) ANNUAL REPORT.—The Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives an annual report on the status and progress of the development of the capabilities described in paragraph (1). Such reports shall be required until such capabilities are fully implemented.

(h) VOLUNTARY INFORMATION SHARING PROCEDURES.—

(1) PROCEDURES.—

(A) IN GENERAL.—The Center may enter into a voluntary information sharing relationship with any consenting non-Federal entity for the sharing of cyber threat indicators and defensive measures for cybersecurity purposes in accordance with this section. Nothing in this subsection may be construed to require any non-Federal entity to enter into any such information sharing relationship with the Center or any other entity. The Center may terminate a voluntary information sharing relationship under this subsection, at the sole and unreviewable discretion of the Secretary, acting through the Director, for any reason, includ-

ing if the Center determines that the non-Federal entity with which the Center has entered into such a relationship has violated the terms of this subsection.

(B) NATIONAL SECURITY.—The Secretary may decline to enter into a voluntary information sharing relationship under this subsection, at the sole and unreviewable discretion of the Secretary, acting through the Director, for any reason, including if the Secretary determines that such is appropriate for national security.

(2) VOLUNTARY INFORMATION SHARING RELATIONSHIPS.—A voluntary information sharing relationship under this subsection may be characterized as an agreement described in this paragraph.

(A) STANDARD AGREEMENT.—For the use of a non-Federal entity, the Center shall make available a standard agreement, consistent with this section, on the Department's website.

(B) NEGOTIATED AGREEMENT.—At the request of a non-Federal entity, and if determined appropriate by the Center, at the sole and unreviewable discretion of the Secretary, acting through the Director, the Department shall negotiate a non-standard agreement, consistent with this section.

(C) EXISTING AGREEMENTS.—An agreement between the Center and a non-Federal entity that is entered into before the date of enactment of this subsection, or such an agreement that is in effect before such date, shall be deemed in compliance with the requirements of this subsection, notwithstanding any other provision or requirement of this subsection. An agreement under this subsection shall include the relevant privacy protections as in effect under the Cooperative Research and Development Agreement for Cybersecurity Information Sharing and Collaboration, as of December 31, 2014. Nothing in this subsection may be construed to require a non-Federal entity to enter into either a standard or negotiated agreement to be in compliance with this subsection.

(i) DIRECT REPORTING.—The Secretary shall develop policies and procedures for direct reporting to the Secretary by the Director of the Center regarding significant cybersecurity risks and incidents.

(j) REPORTS ON INTERNATIONAL COOPERATION.—Not later than 180 days after the date of enactment of this subsection, and periodically thereafter, the Secretary of Homeland Security shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the range of efforts underway to bolster cybersecurity collaboration with relevant international partners in accordance with subsection (c)(8).

(k) OUTREACH.—Not later than 60 days after the date of enactment of this subsection, the Secretary, acting through the Director, shall—

(1) disseminate to the public information about how to voluntarily share cyber threat indicators and defensive measures with the Center; and

(2) enhance outreach to critical infrastructure owners and operators for purposes of such sharing.

(l) CYBERSECURITY OUTREACH.—

(1) IN GENERAL.—The Secretary may leverage small business development centers to provide assistance to small business concerns by disseminating information on cyber threat indicators, defense measures, cybersecurity risks, incidents, analyses, and warnings to help small business concerns in developing or enhancing cybersecurity infrastructure, awareness of cyber threat indicators, and cyber training programs for employees.

(2) DEFINITIONS.—For purposes of this subsection, the terms "small business concern" and "small business development center" have the meaning given such terms, respectively, under section 3 of the Small Business Act.

(m) COORDINATED VULNERABILITY DISCLOSURE.—The Secretary, in coordination with industry and other stakeholders, may develop and adhere to Department policies and procedures for coordinating vulnerability disclosures.

(n) PROTOCOLS TO COUNTER CYBERSECURITY VULNERABILITIES.—The Director may, as appropriate, identify, develop, and disseminate actionable protocols to mitigate cybersecurity vulnerabilities, including in circumstances in which such vulnerabilities exist because software or hardware is no longer supported by a vendor.

* * * * * * *

○