116TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
116–89

DHS CYBER INCIDENT RESPONSE TEAMS ACT OF 2019

MAY 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. 1158]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 1158) to authorize cyber incident response teams at the Department of Homeland Security, 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. 1158, THE "DHS CYBER INCIDENT RESPONSE TEAMS ACT OF 2019"

The purpose of H.R. 1158, the *Cyber Incident Response Teams Act of 2019*, is to authorize cyber incident response teams at the

Department of Homeland Security. H.R. 1158 codifies the cyber incident response teams at the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Located within the National Cybersecurity and Communications Integration Center (NCCIC), the cyber incident response teams will provide—upon request—assistance to asset owners and operators following a cyber incident. H.R. 1158 authorizes DHS to leverage private sector cybersecurity resources to build capacity. H.R. 1158 further directs the NCCIC to continually assess and evaluate the cyber incident response teams and their operations and to periodically provide to Congress the collected information on the metrics used for evaluation and assessment of the cyber response teams and operations.

BACKGROUND AND NEED FOR LEGISLATION

DHS's NCCIC currently utilizes cyber incident response expertise in several ways. The United States Computer Emergency Readiness Team (US–CERT), operated within the NCCIC, brings advanced network and digital media analysis expertise to bear on malicious activity targeting our nation's networks. USCERT develops timely and actionable information for distribution to Federal departments and agencies, state and local governments, private sector organizations, and international partners. The critical mission activities of US–CERT's include: providing cybersecurity protection to Federal civilian executive branch agencies; responding to incidents and analyzing data about emerging cyber threats; and collaborating with foreign governments and international entities to enhance the nation's cybersecurity posture.

The NCCIC's cyber incident teams, known as Hunt and Incident Response Teams (HIRT), provide onsite incident response, free of charge, to organizations that require immediate investigation and resolution of cyber-attacks. These teams provide DHS's front-line response for cyber incidents and proactively hunting for malicious cyber activity. Upon notification of a cyber incident, HIRT will perform a preliminary diagnosis to determine the extent of the compromise. When requested, HIRT can deploy a team to meet with the affected organization to review network topology, identify infected systems and collect other data as needed to perform thorough follow on analysis. They also can provide mitigation strategies and assist asset owners and operators in restoring service and provide recommendations for improving overall network and control systems security. If enacted, H.R. 1158 would codify the work of US–CERT and the HIRT while providing DHS flexibility to also call upon outside expertise.

HEARINGS

The Committee did not hold any hearings on H.R. 1158, however the following hearings informed the Committee on this legislation.

The Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation on April 30, 2019 entitled "Resourcing DHS' Cybersecurity and Innovation Missions: A Review of the Fiscal Year 2020 Budget Request for the Cybersecurity and Infrastructure Security Agency and the Science and Technology Directorate." The Honorable Christopher Krebs, Director, Cybersecurity and Infrastructure

Security Agency, U.S. Department of Homeland Security and testified about CISA's ability to provide cybersecurity services.

During the 115th Congress, the Subcommittee on Cybersecurity and Infrastructure Protection held a joint hearing with the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services on November 14, 2018, entitled "Interagency Cyber Cooperation: Roles, Responsibilities and Authorities of the Department of Defense & the Department of Homeland Security." Testimony was heard from Ms. Jeanette Manfra, Assistant Secretary for the Office of Cybersecurity and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security, The Honorable Kenneth P. Rapuano, Assistant Secretary of Defense for Homeland Defense and Global Security, U.S. Department of Defense, Lieutenant General Bradford J. Shwedo, USAF, Director for Command, Control, Communications and Computers/Cyber, Chief Information Officer, U.S. Department of Defense.

The Subcommittee on Cybersecurity and Infrastructure Protection held a hearing on July 25, 2018, entitled "Assessing the State of Federal Cybersecurity Risk Determination." Testimony was heard from Mr. Ken Durbin, Senior Strategist, Global Government Affairs, Symantec, Ms. Summer C. Fowler, Technical Director, Cybersecurity Risk and Resilience, Software Engineering Institute CERT, Carnegie Mellon University, Mr. Ari Schwartz, Managing Director of Cybersecurity Services, Cybersecurity Risk Management Group, Venable LLP—Testifying on behalf of the Cybersecurity Coalition and Center for Cybersecurity Policy and Law.

COMMITTEE CONSIDERATION

The Committee met on May 15, 2019, with a quorum being present, to consider H.R. 1158 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.

No recorded votes were requested during consideration of H.R. 1158.

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 estimate of the estimate of new budget authority, entitlement authority, or tax expenditures or revenues contained in the cost estimate prepared by the Director of the Congressional Budget Office.

H.R. 1158, DHS Cyber Incident Response Teams Act of 2019
As ordered reported by the House Committee on Homeland Security on May 15, 2019

By Fiscal Year, Millions of Dollars	2019	2019-2024	2019-2029
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Deficit Effect	0	0	0
Spending Subject to Appropriation (Outlays)	*	*	*

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

* = between zero and $500,000.

H.R. 1158 would codify the establishment of hunt and incident response teams (HIRTs) under the authority of the National Cybersecurity and Communications Integration Center (NCCIC) in the Department of Homeland Security (DHS). Under the bill, HIRTs would continue to provide assistance to federal and nonfederal entities affected by malicious cyber activity. The bill also would require the NCCIC to report to the Congress on HIRT operations at the end of each of the first four fiscal years following the bill's enactment.

On the basis of information from DHS and considering information about similar reporting requirements, CBO estimates that enacting H.R. 1158 would cost less than $500,000 over the 2019–2024 period; such spending would be subject to the availability of appropriated funds.

On February 19, 2019, CBO transmitted a cost estimate for S. 315, the DHS Cyber Hunt and Incident Response Teams Act of 2019 as ordered reported by the Senate Committee on Homeland Security and Governmental Affairs. The two bills are similar and CBO's estimates of their costs are the same.

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 estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 1158 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. 1158 would require authorize the Department of Homeland Security to fulfill its cybersecurity mission by providing support for Federal agencies and owners and operators of critical infrastructure affected by cybersecurity incidents.

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 this bill may be cited as the "DHS Cyber Incident Response Teams Act of 2019".

Sec. 2. Department of Homeland Security cyber incident response teams

This section amends the section 2209 of the Homeland Security Act of 2002 to formally codify the NCCIC's cyber incident response teams. These teams can provide, as appropriate and upon request, assistance to owners and operators following a cyber-incident; identification of cyber risk and unauthorized cyber activity; risk management and mitigation strategies for private sector entities; overall recommendations for network and system controls; and other capabilities that may be deemed appropriate. The authorization measure reflects the Committee's continued support for the work of these important teams.

This section also authorizes the DHS Secretary to utilize private sector cybersecurity specialists on the cyber hunt and incident response teams. The Committee intends for the cyber hunt and incident response teams to work hand-in-hand with private sector cybersecurity specialists, when appropriate. The Committee intends for this provision to increase the talent pool from which DHS can draw to continue to accomplish the Department's cybersecurity mission. This section requires the NCCIC to continually assess and assign metrics to the cyber incident response team's operations.

This section requires the Center to submit to the Committee on Homeland Security of the House and Committee on Homeland Security and Governmental Affairs of the Senate, for the first four years after the enactment of this bill, information on the activities of these teams. The NCCIC is required to provide information on metrics, the total number of incident response requests received, the number of incident response tickets opened, all interagency

staffing of incident response teams, and the interagency collaborations established to support incident response teams. No additional funds are authorized to carry out the requirements of this Act.

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 "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 the Cybersecurity and Infrastructure Security Agency. The head of the Center shall report to the Assistant Director 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, defensive measures, cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities, including the implementation of title I of the Cyber security 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, defensive measures, cybersecurity risks, and incidents; and

(B) sharing the analysis conducted under subparagraph (A) 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, cyber security risks, 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 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, 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*, including cybersecurity specialists*;

(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.

(f) CYBER INCIDENT RESPONSE TEAMS.—

(1) IN GENERAL.—The Center shall maintain cyber hunt and incident response teams for the purpose of providing, as appropriate and upon request, assistance, including the following:

(A) Assistance to asset owners and operators in restoring services following a cyber incident.

(B) The identification of cybersecurity risk and unauthorized cyber activity.

(C) Mitigation strategies to prevent, deter, and protect against cybersecurity risks.

(D) Recommendations to asset owners and operators for improving overall network and control systems security to lower cybersecurity risks, and other recommendations, as appropriate.

(E) Such other capabilities as the Under Secretary appointed under section 103(a)(1)(H) determines appropriate.

(2) CYBERSECURITY SPECIALISTS.—The Secretary may include cybersecurity specialists from the private sector on cyber hunt and incident response teams.

(3) ASSOCIATED METRICS.—The Center shall continually assess and evaluate the cyber incident response teams and their operations using robust metrics.

(4) SUBMITTAL OF INFORMATION TO CONGRESS.—Upon the conclusion of each of the first four fiscal years ending after the date of the enactment of this subsection, the Center shall submit to the Committee on Homeland Security of the House of Representatives and the Homeland Security and Governmental Affairs Committee of the Senate, information on the metrics used for evaluation and assessment of the cyber incident response teams and operations pursuant to paragraph (3), including the resources and staffing of such cyber incident response teams. Such information shall include each of the following for the period covered by the report:

(A) The total number of incident response requests received.

(B) The number of incident response tickets opened.

(C) All interagency staffing of incident response teams.

(D) The interagency collaborations established to support incident response teams.

(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)] *(g)* NO RIGHT OR BENEFIT.—

(1) IN GENERAL.—The provision of assistance or information to, and inclusion in the Center*, or any team or activity of 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*, or any team or activity of 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)] *(h)* 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)] *(i)* 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 sub-

section, at the sole and unreviewable discretion of the Secretary, acting through the Director, for any reason, including 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)**]** *(j)* 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)**]** *(k)* 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)**]** *(l)* 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)] *(m)* 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)] *(n)* 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.

* * * * * * *

○