Calendar No. 62

116TH CONGRESS
1st Session

SENATE

REPORT
116–27

DHS CYBER HUNT AND INCIDENT RESPONSE TEAMS ACT OF 2019

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 315

TO AUTHORIZE CYBER HUNT AND INCIDENT RESPONSE TEAMS AT THE DEPARTMENT OF HOMELAND SECURITY, AND FOR OTHER PURPOSES

APRIL 8, 2019.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
89–010 WASHINGTON : 2019

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
MICHAEL B. ENZI, Wyoming
JOSH HAWLEY, Missouri

GARY C. PETERS, Michigan
THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KAMALA D. HARRIS, California
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada

GABRIELLE D'ADAMO SINGER, *Staff Director*
JOSEPH C. FOLIO, III, *Chief Counsel*
COLLEEN E. BERNY, *Professional Staff Member*
DAVID M. WEINBERG, *Minority Staff Director*
ZACHARY I. SCHRAM, *Minority Chief Counsel*
ALEXA E. NORUK, *Minority Director of Homeland Security*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 62

116TH CONGRESS, *1st Session* | SENATE | REPORT 116–27

DHS CYBER HUNT AND INCIDENT RESPONSE TEAMS ACT OF 2019

APRIL 8, 2019.—Ordered to be printed

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

R E P O R T

[To accompany S. 315]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 315) to authorize cyber hunt incident response teams at the Department of Homeland Security, 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

The purpose of S. 315, the Department of Homeland Security Cyber Hunt and Incident Response Teams Act of 2019, is to authorize the Department of Homeland Security (DHS, or the Department) to maintain cyber hunt and incident response teams (teams), codify an existing program within the Department, and foster public-private cooperation. The legislation instructs the Department to ensure that the teams assist in protecting infrastructure from cyber threats and help restore the functionality of private or public infrastructure following a cyberattack. The teams must also iden-

tify cybersecurity risks, develop mitigation strategies, and provide guidance to infrastructure owners.

The bill helps build public-private partnerships by authorizing the Department to include private cybersecurity specialists on the teams. To help inform the Congress about the extent to which the teams are effective in accomplishing their mission and whether the Department was effectively mitigating cybersecurity risk, the Department must maintain metrics that are quantifiable, actionable, can make the teams more effective, and provide reports to the appropriate Congressional committees.[1]

II. Background and Need For the Legislation

In 2009, the Department created the National Cybersecurity and Communications Integration Center (NCCIC) to coordinate and streamline the nation's response to cyber threats.[2] The National Cybersecurity Protection Act of 2014 and the amendment by the Cybersecurity Act of 2015 authorized the NCCIC to "receive, analyze, and disseminate information about cybersecurity risks and incidents and to provide guidance, assessments, incident response support, and other technical assistance upon request."[3]

In an effort to advance these responsibilities, the NCCIC combined the incident response capabilities within the United States Computer Emergency Readiness Team and the Industrial Control Systems Computer Emergency Response Team, to form the Hunt and Incident Response Team (HIRT).[4] The goal of HIRT is to provide "onsite incident response, free of charge, to organizations that require immediate investigation and resolution of cyber-attacks."[5] According to the NCCIC:

> Upon notification of a cyber incident, HIRT will perform a preliminary diagnosis to determine the extent of the compromise. At the customer's request, HIRT can deploy a team to meet with the affected organization to review network topology, identify infected systems, image drives for analysis, and collect other data as needed to perform thorough follow on analysis. HIRT is able to provide mitigation strategies and assist asset owners/operators in restoring service and provide recommendations for improving overall network and control systems security.[6]

During the 115th Congress, the Committee held hearings regarding cyber threats facing the United States and the need to mitigate the nation's cybersecurity risk. In May 2017, Mr. Stephen Chabinsky, a former official with the Federal Bureau of Investiga-

---

[1] On September 26, 2018, the Committee approved S. 3309, DHS Cyber Incident Response Teams Act of 2018. That bill is substantially similar to S. 315. Accordingly, this committee report is in large part a reproduction of Chairman Johnson's committee report for S. 3309, S. Rep. No. 115-412.

[2] Press Release, Dep't of Homeland Sec., Secretary Napolitano Opens New National Cybersecurity and Communications Integration Center (Oct. 30, 2009), *available at* https://www.dhs.gov/news/2009/10/30/new-national-cybersecurity-center-opened.

[3] Dep't of Homeland Sec., U.S. Department of Homeland Security Cybersecurity Strategy (May 15, 2018), *available at* https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_0.pdf.

[4] *See* Dep't of Homeland Sec., Nat'l Cybersecurity & Commc'ns Integration Ctr., NCCIC Fact Sheet (last accessed Mar. 12, 2019), *available at* https://ics-cert.us-cert.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_NCCIC%20ICS_S508C.pdf.

[5] *Id.*

[6] *Id.*

tion and a cybersecurity expert, testified before the Committee and described the cybersecurity landscape in stark terms:

> The cyber threat is real and growing. Our vulnerabilities are real and growing. Our reliance on technology is real and growing. The harm from cyber-attacks is real and growing. Government agency cyber risk is real and growing. The risk to our national security is real and growing. The amount of time, money, and talent that our country is diverting from other issues and devoting to cybersecurity is real and growing. All of these problems are real and growing, and they are getting worse.[7]

The Committee also heard testimony about the role that the Department of Homeland Security plays in addressing national cybersecurity risk. In April 2018, Jeanette Manfra, Assistant Secretary, Office of Cybersecurity and Communications, with the former National Protection and Programs Directorate (NPPD), now the Cybersecurity and Infrastructure Security Agency, testified about their role:

> We endeavor to enhance cyber threat information-sharing across the globe to stop cyber incidents before they start and help businesses and government agencies to protect their cyber systems and quickly recover should such an attack occur.[8]

Gregory Wilshusen, Director of Information Security Issues at the Government Accountability Office, testified about the Department's need to "enhance efforts to improve and promote the security of federal and private sector networks."[9] Mr. Wilshusen described opportunities for the NCCIC to enhance its work to support national cybersecurity:

> [T]he extent to which the [NCCIC] had performed its required functions in accordance with statutorily defined implementing principles was unclear, in part, because the [NCCIC] had not established metrics and methods by which to evaluate its performance against the principles. Further, in its role as the lead federal agency for collaborating with eight critical infrastructure sectors including the communications and dams sectors, DHS had not developed metrics to measure and report on the effectiveness of its cyber risk mitigation activities or on the cybersecurity posture of the eight sectors.[10]

S. 315 codifies the Department's cyber hunt and incident response teams and requires the NCCIC to assess the cyber incident

---

[7] *Cyber Threats Facing America: An Overview of the Cybersecurity Threat Landscape: Hearing before S. Comm. on Homeland Sec. & Governmental Affairs* 115th Cong. (2017) (statement of Steven Chabinsky, Global Chair of Data, Privacy, and Cyber Security, White & Case LLP), https://www.hsgac.senate.gov/imo/media/doc/Testimony-Chabinsky-2017-05-10-REVISED.pdf.

[8] *Mitigating America's Cybersecurity Risk: Hearing before S. Comm. on Homeland Sec. & Governmental Affairs* 115th Cong. (2018) (statement of Jeanette Manfra, Assistant Sec., Office of Cybersecurity & Communications, Nat'l Programs & Prot. Directorate, U.S. Dep't of Homeland Sec.), *available at* https://www.hsgac.senate.gov/imo/media/doc/Testimony-Manfra-2018-04-24.pdf.

[9] *Id.* (statement of Gregor Wilshusen, Director of Information Security Issues, U.S. Gov't Accountability Office), *available at* https://www.hsgac.senate.gov/imo/media/doc/Testimony-Wilshusen-2018-04-24.pdf.

[10] *Id.*

response teams and their operations. The legislation also requires the NCCIC to define the teams' goals and outcomes, and develop appropriate metrics. These metrics must be quantifiable, actionable, and improve the overall effectiveness and accountability of the teams. A report to the appropriate congressional committees on the metrics and additional data on the teams' performance is required for each of the first four fiscal years after date of enactment. The combinations of these metrics and reporting will help Congress better understand the team's and NCCIC's ability to mitigate national cybersecurity risk.

III. Legislative History

Senators Margaret Wood Hassan (D–NH) and Rob Portman (R–OH) introduced S. 315 on January 31, 2019. The bill was referred to the Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 315 at a business meeting on February 13, 2019. Senator Hassan offered a substitute amendment that made technical changes, required the Department to define the teams' goals and desired outcomes, and further clarified the evaluation metrics, including requiring the Department to develop appropriate metrics that are quantifiable and actionable. The Committee adopted the substitute amendment and ordered the bill, as amended, reported favorably by voice vote *en bloc*. Senators present for both the vote on the substitute amendment and the vote on the bill as amended were: Johnson, Portman, Paul, Lankford, Romney, Scott, Enzi, Hawley, Peters, Carper, Hassan, Harris, Sinema, and Rosen.

IV. Section-by-Section Analysis of the Bill, as Reported

Section 1. Short title

This section provides the bill's short title, the "DHS Cyber Hunt and Incident Response Teams Act of 2019."

Section 2. Department of Homeland Security cyber hunt incident response teams

Subsection (a) amends the Homeland Security Act to allow DHS to include private sector cybersecurity specialists in the composition of entities and persons at the NCCIC, as well as members of cyber hunt and incident response teams.

The subsection further authorizes the NCCIC to maintain cyber hunt and incident response teams to provide assistance upon request for specific purposes. The legislation authorizes the teams to provide cybersecurity response and technical assistance, upon request, to Federal and non-Federal entities. The types of assistance can include, "restoring services following a cyber incident"; "identification of cybersecurity risk and unauthorized cyber activity"; "mitigation strategies to prevent, deter, and protect against cybersecurity risks"; and "recommendations to asset owners and operators for improving overall network and control systems security to lower cybersecurity risks".

This subsection also requires the NCCIC to define the goals and outcomes for the teams and develop metrics. The metrics are required to be quantifiable, actionable, and be used to improve the teams' overall effectiveness and accountability. The subsection also

states that the Secretary may include private sector cybersecurity specialists on the teams after providing notice to a requesting entity, and with their approval.

Subsection (b) requires a yearly report to the appropriate Congressional Committees evaluating the teams, including incident data and interagency staffing information.

Subsection (c) states that no additional funds are authorized by the legislation.

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, February 19, 2019.

Hon. Ron Johnson, *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. 315, the DHS Cyber Hunt and Incident Response Teams Act of 2019.

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

Sincerely,

Keith Hall,
Director.

Enclosure.

S. 315, DHS Cyber Hunt and Incident Response Teams Act of 2019

As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on February 13, 2019

Millions of Dollars	Direct Spending	Revenues	Net Deficit Effect	Spending Subject to Appropriation
2019	0	0	0	*
2019-2024	0	0	0	*
2019-2029	0	0	0	n.a.

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 $0 and $500,000; n.a. = not applicable.

S. 315 would codify the role and responsibilities of existing 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.

S. 315 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 S. 315 would cost less than $500,000 over the 2019–2024 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 Assistant Director for 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 S. 315 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):

HOMELAND SECURITY ACT OF 2002

* * * * * * *

TITLE II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

* * * * * * *

Subtitle B—Critical Infrastructure Information

* * * * * * *

SEC. 227. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

* * * * * * *

(a) * * *

* * * * * * *

(d) COMPOSITION.—

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

(A) * * *

(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*;

* * * * * * *

(e) * * *

(f) CYBER HUNT AND INCIDENT RESPONSE TEAMS.—

(1) IN GENERAL.—The Center shall maintain cyber hunt and incident response teams for the purpose of leading Federal asset response activities and providing timely technical assistance to Federal and non-Federal entities, including across all critical infrastructure sectors, regarding actual or potential security incidents, as appropriate and upon request, including—

(A) assistance to asset owners and operators in restoring services following a cyber incident;

(B) identification and analysis 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; and

(E) such other capabilities as the Secretary determines appropriate.

(2) ASSOCIATED METRICS.—The Center shall—

(A) define the goals and desired outcomes for each cyber hunt and incident response team; and

(B) develop metrics—

(i) to measure the effectiveness and efficiency of each cyber hunt and incident response team in achieving the goals and desired outcomes defined under subparagraph (A); and

(ii) that—

(I) are quantifiable and actionable; and

(II) the Center shall use to improve the effectiveness and accountability of, and service delivery by, cyber hunt and incident response teams.

(3) CYBERSECURITY SPECIALISTS.—After notice to, and with the approval of, the entity requesting action by or technical assistance from the Center, the Secretary may include cybersecurity specialists from the private sector on a cyber hunt and incident response team.

[f**]***(g)* NO RIGHT OR BENEFIT.—

(1) IN GENERAL.—The provision of assistance or information to, and inclusion in the Center, o*r 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 Under Secretary appointed under section 103(a)(1)(H).

(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.—

* * * * * * *

[h**]***(i)* VOLUNTARY INFORMATION SHARING PROCEDURES.—

* * * * * * *

[i**]***(j)* DIRECT REPORTING.—* * *

[j**]***(k)* REPORTS ON INTERNATIONAL COOPERATION.—* * *

[k**]***(l)* OUTREACH.—* * *

* * * * * * *

[l**]***(m)* CYBERSECURITY OUTREACH.—

* * * * * * *

[m**]***(n)* COORDINATED VULNERABILITY DISCLOSURE.—* * *

* * * * * * *

○