Calendar No. 716

115TH CONGRESS *2d Session*	SENATE	REPORT 115–412

DHS CYBER INCIDENT RESPONSE TEAMS ACT OF 2018

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 3309

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

DECEMBER 4, 2018.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE

89–010 WASHINGTON : 2018

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MICHAEL B. ENZI, Wyoming
JOHN HOEVEN, North Dakota
STEVE DAINES, Montana
JON KYL, Arizona

CLAIRE MCCASKILL, Missouri
THOMAS R. CARPER, Delaware
HEIDI HEITKAMP, North Dakota
GARY C. PETERS, Michigan
MAGGIE HASSAN, New Hampshire
KAMALA D. HARRIS, California
DOUG JONES, Alabama

CHRISTOPHER R. HIXON, *Staff Director*
GABRIELLE D'ADAMO SINGER, *Chief Counsel*
MICHELLE D. WOODS, *Senior Professional Staff Member*
MARGARET E. DAUM, *Minority Staff Director*
CHARLES A. MOSKOWITZ, *Minority Senior Legislative Counsel*
SUBHASRI RAMANATHAN, *Minority Counsel*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 716

115TH CONGRESS, *2d Session* | SENATE | REPORT 115–412

DHS CYBER INCIDENT RESPONSE TEAMS ACT OF 2018

DECEMBER 4, 2018.—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. 3309]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 3309) to authorize cyber 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

		Page
I.	Purpose and Summary	1
II.	Background and Need for the Legislation	2
III.	Legislative History	4
IV.	Section-by-Section Analysis	4
V.	Evaluation of Regulatory Impact	5
VI.	Congressional Budget Office Cost Estimate	5
VII.	Changes in Existing Law Made by the Bill, as Reported	6

I. PURPOSE AND SUMMARY

The purpose of S. 3309, the Department of Homeland Security Cyber Incident Response Teams Act of 2018, is to authorize 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 identify 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 and provide reports to the appropriate Congressional committees.

II. Background and the Need for 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.[1] 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."[2]

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).[3] The goal of HIRT is to provide "onsite incident response, free of charge, to organizations that require immediate investigation and resolution of cyber-attacks."[4] 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.[5]

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 Investigation 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 grow-

---

[1] 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.

[2] 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.

[3] *See* Dep't of Homeland Sec., National Cybersecurity and Communications Integration Center, NCCIC Fact Sheet (last accessed Nov. 20, 2018), *available at* https://ics-cert.us-cert.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_NCCIC%20ICS_S508C.pdf.

[4] *Id.*

[5] *Id.*

> ing. 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.[6]

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 National Protection and Programs Directorate (NPPD), testified about NPPD's 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.[7]

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."[8] 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.[9]

S. 3309 codifies the Department's cyber hunt and incident response teams and requires the NCCIC to assess the cyber incident response teams and their operations. The legislation also requires the NCCIC to report to congressional committees annually about these teams and provide data about their performance. The combinations of these metrics and annual reporting will help Congress better understand the team's and NCCIC's ability to mitigate national cybersecurity risk.

---

[6] *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.

[7] *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.

[8] *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.

[9] *Id.*

III. LEGISLATIVE HISTORY

Senators Margaret Wood Hassan (D–NH) and Rob Portman (R–OH) introduced S. 3309 on July 13, 2018. The bill was referred to the Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 3309 at a business meeting on September 26, 2018. Senator Hassan offered a substitute amendment and a modification to the substitute amendment that clarify the Department's responsibility for Federal asset response and for providing technical assistance to non-Federal entities and critical infrastructure sectors. Additionally, the modified substitute amendment authorizes the Department to use private sector cybersecurity specialists, upon notice and approval of the Secretary, on cyber incident and response teams. The Committee adopted the amendment as modified and ordered the bill, as amended, reported favorably, both by voice vote. Senators present for both the vote on the modified amendment and the vote on the underlying bill were: Johnson, Portman, Lankford, Enzi, Hoeven, McCaskill, Carper, Heitkamp, Peters, Hassan, Harris, and Jones.

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 Incident Response Teams Act of 2018."

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 requires the NCCIC to assess and evaluate cyber incident response teams and their operations using "robust metrics." The subsection also requires NCCIC to submit a report to Congress annually for the first four fiscal years following the legislation's enactment. The annual report should reflect the assessment, evaluation, and robust metrics obtained by DHS and the NCCIC.

Subsection (b) 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, October 9, 2018.

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. 3309, the DHS Cyber Incident Response Teams Act of 2018.

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

Sincerely,

Keith Hall,
Director.

Enclosure.

S. 3309—DHS Cyber Incident Response Teams Act of 2018

S. 3309 would codify the establishment and responsibilities 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.

S. 3309 also would require the NCCIC to report to the Congress on HIRTs' activities at the end of each of the first four fiscal years following the bill's enactment. Using information from DHS and considering information about similar reporting requirements, CBO estimates that implementing S. 3309 would cost less than $500,000 over the 2019–2023 period; such spending would be subject to the availability of appropriated funds.

Enacting S. 3309 would not affect direct spending or revenues; therefore, pay-as-you-go procedures do not apply.

CBO estimates that enacting S. 3309 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2029.

S. 3309 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act.

On March 15, 2018, CBO transmitted a cost estimate for H.R. 5074, the DHS Cyber Incident Response Teams Act of 2018, as ordered reported by the House Committee on Homeland Security on

March 7, 2018. The two pieces of legislation are similar and the estimated budgetary effects are the same.

The CBO staff contact for this estimate is William Ma. 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. 3309 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 continually assess and evaluate the cyber hunt and incident response teams and the operations of those cyber hunt and incident response teams using robust metrics.

(3) REPORT.—At the conclusion of each of the first 4 fiscal years after the date of the enactment of the DHS Cyber Incident Response Teams Act of 2018, the Center shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report that includes—

(A) information relating to the metrics used for evaluation and assessment of the cyber hunt and incident response teams and operations under paragraph (2), including the resources and staffing of those cyber hunt and incident response teams; and

(B) for the period covered by the report—

(i) the total number of incident response requests received;

(ii) the number of incident response tickets opened; and

(iii) a statement of—

(I) all interagency staffing of cyber hunt and incident response teams; and

(II) the interagency collaborations established to support cyber hunt and incident response teams.

(4) 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*, 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 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.— * * *

* * * * * * *

○