Calendar No. 36

116TH CONGRESS
1st Session

SENATE

REPORT
116–5

NATIONAL CYBERSECURITY PREPAREDNESS CONSORTIUM ACT OF 2019

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 333

TO AUTHORIZE THE SECRETARY OF HOMELAND SECURITY TO WORK WITH CYBERSECURITY CONSORTIA FOR TRAINING, AND FOR OTHER PURPOSES

MARCH 12, 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*
MICHAEL J.R. FLYNN, *Senior Counsel*
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. 36

116TH CONGRESS *1st Session* | SENATE | REPORT 116–5

NATIONAL CYBERSECURITY PREPAREDNESS CONSORTIUM ACT OF 2019

MARCH 12, 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. 333]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 333), to authorize the Secretary of Homeland Security to work with cybersecurity consortia for training, and for other purposes, having considered the same, reports favorably thereon without amendment and recommends that the bill do pass.

CONTENTS

I. PURPOSE AND SUMMARY

The purpose of S. 333, the National Cybersecurity Preparedness Consortium Act of 2019, is to codify the Secretary of Homeland Security's existing authority to work with consortia, primarily composed of academic institutions and nonprofit entities with expertise in cybersecurity, to address cybersecurity risks and incidents. The Secretary may work with a consortium to provide assistance to the National Cybersecurity and Communications Integration Center (NCCIC) within the Department of Homeland Security (DHS) to

provide cybersecurity related training and expertise to state and local first responders and critical infrastructure owners and operators.[1]

II. BACKGROUND AND THE NEED FOR LEGISLATION

The Committee recognizes the challenges DHS faces in fulfilling its cyber mission and implementing timely and effective measures to mitigate the security risks posed by nefarious cyber incidents.[2] Specifically, DHS is responsible for coordinating the Federal Government's efforts to protect the nation's critical infrastructure.[3] In April 2018, the Committee held a hearing entitled, *Mitigating America's Cybersecurity Risks,* to discuss the risks posed by malicious cyber incidents and to assess how DHS is using its existing authorities and cyber capabilities to minimize security risks.[4] Currently, 85 percent of the United States' national critical infrastructure is owned by private entities.[5]

The combination of the cybersecurity manpower shortage and the majority of our nation's critical infrastructure being in private hands has created a unique public-private environment for DHS to operate in.[6] The Committee held a hearing in June 2017 entitled, *Cybersecurity Regulation Harmonization,* to highlight the importance of public-private partnerships in combating cyber challenges facing DHS. Witness Dean Garfield provided written testimony that stated: "Congress should consider the public and private sectors' ongoing collaboration and efforts to implement pre-existing regulations before further legislating on cybersecurity so that Members may arrive at a holistic, federal cybersecurity strategy approach."[7]

During the Committee's April 2018 hearing on mitigating cybersecurity risks, the DHS Assistant Secretary for Cybersecurity and Communications, Janette Manfra, testified that DHS has "taken steps to empower public and private partners to defend against many of these threats by publicly attributing state-sponsored activity, issuing technical indicators and providing mitigation guidance."[8] For example, DHS has partnered with universities to aid in cyber security training.[9] In 2004, DHS began partnering with

---

[1] On September 26, 2018, the Committee approved S. 594, the National Cybersecurity Preparedness Consortium Act of 2018. That bill is substantially similar to S. 333. Accordingly, this committee report is in large part a reproduction of Chairman Johnson's committee report for S. 594, S. Rep. No. 115–410.

[2] *Mitigating America's Cybersecurity Risks: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs,* 115th Cong. (2018) (statement of Sen. Ron Johnson, R-WI., Chairman), *available at* https://www.hsgac.senate.gov/imo/media/doc/Opening%20Statement-Johnson-2018-04-24.pdf [hereinafter, *Mitigating America's Cybersecurity Risks*].

[3] Press Release, Dep't of Homeland Sec., The Department's Five Responsibilities (June 8, 2009), *available at* https://www.dhs.gov/blog/2009/06/08/departments-five-responsibilities.

[4] *See generally, Mitigating America's Cybersecurity Risks.*

[5] *Critical Infrastructure Protection, Information Sharing and Cyber Security,* U.S. Chamber of Commerce, *available at* https://www.uschamber.com/issue-brief/critical-infrastructure-protection-information-sharing-and-cyber-security (last visited Nov. 6, 2018).

[6] *Id.; see also* U.S. Gov't Accountability Office, GAO–18–466, Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions (June 2018), *available at* https://www.gao.gov/assets/700/692498.pdf.

[7] *Cybersecurity Regulation Harmonization: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs,* 115th Cong. (2017) (statement of Dean Garfield, Pres. and CEO of Info. Tech. Indus. Council), *available at* https://www.hsgac.senate.gov/imo/media/doc/Testimony-Garfield-2017-06-21-REVISED.pdf.

[8] *Mitigating America's Cybersecurity Risks* (statement of Janette Manfra, Assistant Sec'y, Off. of Cybersecurity & Comm., Nat'l Programs Directorate, Dept. of Homeland Sec).

[9] *About,* Nat'l Cyber Security Preparedness Consortium, *available at* http://nationalcpc.org/about.html (last visited Feb. 27, 2019).

the National Cybersecurity Preparedness Consortium.[10] This consortium consists of five university partners from across the United States.[11]

By leveraging the expertise of consortia, DHS can better ensure that its partners in the private sector and state and local governments are prepared to assist the Federal Government in its efforts to combat cyber threats. S. 333 codifies an existing DHS practice and helps strengthen DHS's efforts to partner with the private sector and academia to secure our nation's cyber infrastructure.

III. LEGISLATIVE HISTORY

Senator John Cornyn, (R–TX) introduced S. 333 on February 5, 2019, with Senator Ted Cruz (R–TX) and Senator Patrick Leahy (D–VT).

The Committee considered S. 333 at a business meeting on February 13, 2019. During the business meeting, S. 333 was ordered reported favorably by voice vote *en bloc.* The Senators present for the voice vote 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 established that the bill may be cited as the "National Cybersecurity Preparedness Consortium Act of 2019."

Section 2. Definitions

This section includes definitions of the terms "consortium," "cybersecurity risk," "incident," "Department," and "Secretary."

Section 3. National cybersecurity preparedness consortium

Subsection (a) gives the Secretary the authority to work with a consortium on cyber related issues.

Subsection (b) gives the Secretary guidance on the type of assistance consortia may provide the NCCIC. Under this subsection, consortia may be used to assist in the training of state and local first responders and private industry actors in addressing cybersecurity threats and risks. DHS may also work with consortia to develop and update cybersecurity related emergency plans and to provide technical assistance related to cybersecurity risks and incidents. DHS may also work with the consortia to incorporate cybersecurity incident prevention, risk, and response in existing state and local emergency plans.

Subsection (c) requires the Secretary to consider prior cybersecurity training experience and geographic diversity when selecting consortium participants.

Subsection (d) requires the Secretary to establish metrics for effectiveness of consortium activities.

Subsection (e) requires the Secretary to inform minority-serving institutions of their ability to participate in consortia and support DHS's cybersecurity efforts.

---

[10] *Id.*
[11] *Id.*

Section 4. Rule of construction

This section prohibits the consortium from commanding any law enforcement agency or agents.

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 bill (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 28, 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. 333, the National Cybersecurity Preparedness Consortium 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. 333, National Cybersecurity Preparedness Consortium 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	3
2019-2024	0	0	0	18
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

n.a. = not applicable.

S. 333 would authorize the Department of Homeland Security (DHS) to coordinate with a consortium to assist state and local governments to prepare for and respond to cybersecurity risks. Since 2014, the department has awarded $13 million in grants to members of the National Cybersecurity Preparedness Consortium to de-

liver cybersecurity training and technical assistance to state and local governments. CBO expects that DHS would continue to provide a similar level of support under S. 333. CBO estimates that DHS would provide $3 million in new grant funding each year; such spending would be subject to the availability of appropriated funds. In total, implementing S. 333 would cost $18 million over the 2019–2024 period.

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

Because this legislation would not repeal or amend any provision of current law, it would not make changes in existing law within the meaning of clauses (a) and (b) of paragraph 12 of rule XXVI of the Standing Rules of the Senate.

○