Calendar No. 714

115TH CONGRESS *2d Session*	SENATE	REPORT 115–410

NATIONAL CYBERSECURITY PREPAREDNESS CONSORTIUM ACT OF 2017

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 594

TO AUTHORIZE THE SECRETARY OF HOMELAND SECURITY TO WORK WITH CYBERSECURITY CONSORTIA FOR TRAINING, 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*
JULIE G. KLEIN, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 714

115TH CONGRESS, *2d Session* | SENATE | REPORT 115–410

NATIONAL CYBERSECURITY PREPAREDNESS CONSORTIUM ACT OF 2017

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. 594]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 594), 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 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. 594, the National Cybersecurity Preparedness Consortium Act of 2018, 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 or the Department) to provide cybersecurity related training and exper-

tise to state and local first responders and critical infrastructure owners and operators.

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.[1] Specifically, DHS is responsible for coordinating the Federal Government's efforts to protect the nation's critical infrastructure.[2] 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.[3] During the hearing, Ranking Member Claire McCaskill said "DHS's responsibility also included coordinating critical infrastructure protection. But the majority of the critical infrastructure is not federally owned or operated."[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*, where the importance of public-private partnerships in combating cyber challenges facing DHS was highlighted. Dean Garfield, an expert witness, provided written testimony that stated: "[c]ongress 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 guid-

---

[1] *Hearing on Mitigating America's Cybersecurity Risks 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.

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

[3] *See generally Hearing on Mitigating America's Cybersecurity Risks Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 115th Cong. (2018).

[4] *Hearing on Mitigating America's Cybersecurity Risks Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 115th Cong. (2018) (statement of Sen. Claire McCaskill, D–MO., Ranking Member), *available at* http://www.cq.com/doc/congressionaltranscripts-5304955?0.

[5] Ann M. Beauchesne & Matthew J. Eggers, *Critical Infrastructure Protection, Information Sharing and Cyber Security*, U.S. Chamber of Commerce, (last accessed Nov. 6, 2018), https://www.uschamber.com/issue-brief/critical-infrastructure-protection-information-sharing-and-cybersecurity.

[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 (2018), *available at* https://www.gao.gov/assets/700/692498.pdf.

[7] *Hearing on Cybersecurity Regulation Harmonization 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.

ance."[8] For example, DHS has partnered with universities to aid in cyber security training.[9] In 2004, DHS began partnering with 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. 594 codifies an existing DHS practice and helps strengthen the Department'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. 594 on March 9, 2017, with Senator Ted Cruz (R–TX) and Senator Patrick Leahy (D–VT). Senators John Boozman (R–AR) and Tom Cotton (R–AR) joined as cosponsors on April 6, 2017. The bill was referred to the Committee on March 9, 2017.

The Committee considered S. 594 at a business meeting on September 26, 2018. During the business meeting, Senator Johnson offered a substitute amendment that was accepted by unanimous consent. The substitute amendment narrowed the focus of the collaborative efforts between the Department and a consortium to cybersecurity risks and incidents. It also removed three provisions: a provision that required DHS to work with a specific consortium, a prohibition on duplication of existing program efforts, and the five-year sunset.

The bill, as amended, was ordered reported favorably by voice vote en bloc. The Senators present for the voice vote 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 established that the bill may be cited as the "National Cybersecurity Preparedness Consortium Act of 2018."

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

---

[8] *Hearing on Mitigating America's Cybersecurity Risks, supra* note 1 (statement of Janette Manfra, Assistant Sec'y, Office of Cybersecurity & Communications, Nat'l Programs Directorate, U.S. Dept. of Homeland Sec.).

[9] National Cyber Security Preparedness Consortium, *About*, (last accessed Nov. 20, 2018), http://nationalcpc.org/index.html.

[10] *Id.*

[11] *Id.*

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 the Department's cybersecurity efforts.

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, 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. 594, the National Cybersecurity Preparedness Consortium Act of 2017.

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. 594—National Cybersecurity Preparedness Consortium Act of 2017

S. 594 would authorize the Department of Homeland Security (DHS) to work with a consortium to assist state and local governments to prepare for and respond to cybersecurity risks and incidents. Since 2014, the department has awarded $13 million in

grants to members of the National Cybersecurity Preparedness Consortium to deliver 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. 594. CBO estimates that DHS would provide $3 million in new grant funding each year, assuming appropriation of the estimated amounts. In total, implementing S. 594 would cost $15 million over the 2019–2023 period.

Enacting S. 594 would not affect direct spending or revenues; therefore, pay-as-you-go procedures do not apply.

CBO estimates that enacting S. 594 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2029.

S. 594 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act.

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

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.

○