Calendar No. 526

113TH CONGRESS *2d Session*	SENATE	REPORT 113–240

NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER ACT OF 2014

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 2519

TO CODIFY AN EXISTING OPERATIONS CENTER FOR CYBERSECURITY

JULY 31, 2014.—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE
39–010 WASHINGTON : 2014

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

THOMAS R. CARPER, Delaware, *Chairman*

CARL LEVIN, Michigan
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
CLAIRE MCCASKILL, Missouri
JON TESTER, Montana
MARK BEGICH, Alaska
TAMMY BALDWIN, Wisconsin
HEIDI HEITKAMP, North Dakota

TOM COBURN, Oklahoma
JOHN MCCAIN, Arizona
RON JOHNSON, Wisconsin
ROB PORTMAN, Ohio
RAND PAUL, Kentucky
MICHAEL B. ENZI, Wyoming
KELLY AYOTTE, New Hampshire

GABRIELLE A. BATKIN, *Staff Director*
JOHN P. KILVINGTON, *Deputy Staff Director*
MARY BETH SCHULTZ, *Chief Counsel*
STEPHEN R. VIÑA, *Chief Counsel for Homeland Security*
MATTHEW R. GROTE, *Senior Professional Staff Member*
KEITH B. ASHDOWN, *Minority Staff Director*
CHRISTOPHER J. BARKLEY, *Minority Deputy Staff Director*
ANDREW C. DOCKHAM, *Minority Chief Counsel*
DANIEL P. LIPS, *Minority Director of Homeland Security*
WILLIAM H.W. MCKENNA, *Minority Investigative Counsel*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 526

113TH CONGRESS, *2d Session* | SENATE | REPORT 113–240

NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER ACT OF 2014

JULY 31, 2014.—Ordered to be printed

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

R E P O R T

[To accompany S. 2519]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 2519), to codify an existing operations center for cybersecurity, having considered the same, reports favorably thereon with an amendment and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

S. 2519, the National Cybersecurity and Communications Integration Center Act of 2014, seeks to codify the Department of Homeland Security's existing cybersecurity and communications operations center, known as the National Cybersecurity and Communications Integration Center (NCCIC). Codification would enable DHS to execute its cyber mission more effectively and efficiently.

II. BACKGROUND AND THE NEED FOR LEGISLATION

The United States faces a variety and growing set of sophisticated threats in cyberspace. Cyber criminals, for example, routinely

steal personal identifiable information, as well as trade secrets and financial information from private sector and government networks, resulting in the loss of intellectual property and billions of dollars. For example, a recent indictment brought by the United States Department of Justice of six members of the People's Liberation Army ("PLA"), the military of the People's Republic of China, alleges several cyber attacks through which the defendants stole various trade secrets.[1] One report credibly estimates the likely annual cost to the global economy from cybercrime at more than $400 billion a year.[2] Retired General Keith Alexander, the former Director of the National Security Agency and Commander of U.S. Cyber Command, observed that cyber criminals "are exploiting these targets on a scale amounting to the greatest unwilling transfer of wealth in history."[3]

Some actors in cyberspace seek to disrupt or destroy computer systems, including those that control some of our nation's critical infrastructure—the systems that deliver power and water to our homes, our energy pipelines, our nuclear plants and our telecommunications systems. Cyber attacks on critical infrastructure could potentially lead to massive disruptions, catastrophic economic damage, and, in worst case scenarios, the loss of human life. In Saudi Arabia, for example, a cyber attack against Saudi Aramco, one of the world's largest oil companies, damaged 30,000 computers on the company's network.[4] To date, there has been no similarly damaging cyber attack with physical effects to critical infrastructure in the United States. However, in 2013, major financial institutions were targeted by repeated "denial-of-service" cyber attacks, which attempted to disrupt the performance of company websites by flooding them with internet traffic.[5] Energy and utility companies in the United States have also reportedly been the targets of cyber attacks. For example, DHS has reported a widespread, organized intrusion campaign across the U.S. oil and natural gas sector.[6] While no physical damage was reported, once a malicious actor gains access to a target network, it is not technically difficult to cause disruptions or damage.

The United States has also seen widespread targeting of, theft, and disruption of information stored on the federal government's own networks, where sensitive information, including information related to the operations of critical infrastructure, is at risk of disclosure.[7] For example, the Nuclear Regulatory Commission stored sensitive cybersecurity details for nuclear facilities on an unpro-

---

[1] *United States of America* v. *Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, Gu Chunhui,* http://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf.

[2] McAfee—Intel Security and Center for Strategic and International Studies, "Net Losses: Estimating the Global Cost of Cybercrime" at page 2. (June 2014) http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf (last viewed July 17, 2014).

[3] *Hearing to Receive Testimony on U.S. Strategic Command and U.S. Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2014 and Future Years Defense Programs,* Hearing before the U.S. Senate Committee on Armed Services, Written Statement of General Keith B. Alexander, Commander, U.S. Cyber Command (Mar. 12, 2013).

[4] *See Worldwide Threat Assessment of the US Intelligence Community*, Hearing before the House Permanent Select Committee on Intelligence, Written Statement of James R. Clapper, Director of National Intelligence (April 11, 2013).

[5] *Id.*

[6] *See* ICS–CERT, ICS–CERT *Monthly Monitor*, Department of Homeland Security (April 2012) (online at http://ics-cert.us-cert.gov/monitors).

[7] *See* "The Federal Government's Track Record on Cybersecurity and Critical Infrastructure," Minority Staff Report, U.S. Senate Homeland Security and Governmental Affairs Committee, Sen. Tom Coburn, February 4, 2014.

tected shared drive, making them more vulnerable to malicious cyber actors.[8] In 2011, the Thrift Savings Plan (TSP), the retirement savings and investment plan used by millions of federal employees and members of the uniformed services, suffered a data security breach, allowing unauthorized access to the personal information of approximately 123,000 TSP participants.[9] And, in 2013, malicious actors broke into the computer network at the Department of Energy's Washington headquarters and compromised the personal information of hundreds of employees.[10]

One of the tactics to mitigate the threat of cyber attacks against government networks and the private sector is for the government and private sector partners to share information about cyber security threats, including information about threat signatures, system vulnerabilities, and actions that can be taken to defend networks from attacks. Other tactics include analyzing threat and vulnerability information, and providing technical assistance to industry and other partners.

Within the federal government, the Department of Homeland Security ("DHS" or "the Department") is responsible for working with the private sector to help protect the nation's critical infrastructure from physical and cyber threats and overseeing the protection of the .gov domain. At the center of DHS' cybersecurity and communications mission is the National Cybersecurity and Communications Integration Center (NCCIC). The NCICC is a round-the-clock information sharing, analysis, and incident response center where government, private sector, and international partners work together on cybersecurity matters.

The NCCIC has four components: the United States Computer Emergency Readiness Team (US–CERT), the Industrial Control Systems Cyber Emergency Response Team (ICS–CERT), the National Coordinating Center for Telecommunications (NCC), and Operations Integration. Among its various functions, the NCCIC: analyzes cybersecurity and communications threats and vulnerabilities and coordinates findings with partners to manage risks to critical systems; creates shared situational awareness among public sector, private sector, and international partners by collaboratively developing and sharing timely and actionable cybersecurity and communications information; and responds to cybersecurity and communications incidents and events to mitigate harmful activity, manage crisis situations, and support recovery efforts.

In fiscal year 2013 alone, the NCCIC responded to more than 228,000 incident reports from a variety of stakeholders, ranging from minor compromises of personal information to mass data thefts.[11] The NCCIC also released over 11,000 cyber alerts to industry, federal agencies and other partners in fiscal year 2013, and more than 5,000 organizations have used the NCCIC's tools to per-

---

[8] *See* Nuclear Regulatory Commission, Office of the Inspector General, "Audit of NRC's Shared "S" Drive," (July 27, 2011).

[9] *See* Federal Retirement Thrift Investment Board, Press Release, "Federal Retirement Thrift Investment Board Reports a Cyber Attack on a Contractor Potentially Affecting TSP Participants" (May 25, 2012) https://www.tsp.gov/PDF/formspubs/Press.Release.2012-05-25.Cyber.pdf (last accessed July 20, 2014).

[10] *See* Department of Energy, Office of the Inspector General, The Department of Energy's July 2013 Cyber Security Breach, DOE/IG–0900 (Washington, D.C.: Dec. 6, 2013). http://energy.gov/sites/prod/files/2013/12/f5/IG-0900.pdf (last accessed July 20, 2014).

[11] *Department of Homeland Security, NCCIC Weekly Cyber Analytics Report, Week ending 14 June 2014 (on file with Committee staff).*

form self-assessments to identify their own vulnerabilities. [12] In 2013, NCCIC's ICS–CERT, conducted 76 onsite assessments across critical infrastructure sectors.[13] During the first nine months of Fiscal Year 2014, the NCCIC has received 508,000 reports of incidents, detected over 46,599 vulnerabilities, issued over 9,001 actionable cyber-alerts, and had over 256,003 partners subscribe to its cyber threat warning sharing initiative.[14]

Indeed, the NCCIC has played a major role in addressing a variety of cyber attacks on government and industry networks. For example, less than 24 hours after the NCCIC learned about the "Heartbleed" vulnerability—a weakness in the widely-used OpenSSL encryption software that protects the electronic traffic across much of the internet—the Center released an alert and posted mitigation information on the US–CERT website.[15] During the "denial of service" attacks on U.S. banks in 2012 and 2013 and periodically in 2014, NCCIC's US–CERT provided technical data and assistance to the banks, including identifying 600,000 distributed "denial of service" related internet protocol addresses.[16]

Industry representatives from several sectors of the economy sit on the NCCIC floor. In testimony before the Committee, a representative from the financial industry praised the NCCIC: "[o]ur presence [there] has enhanced situational awareness and information sharing between the financial services sector and the government with numerous examples of success." The witness further stated that the Financial Services Sector Coordinating Council—the entity that coordinates critical infrastructure and homeland security activities in the financial services industry—"supports formalization of the NCCIC through legislation." [17]

The NCCIC currently operates under the Homeland Security Act's general infrastructure protection authorities.[18] S. 2519 seeks to clarify those general existing authorities and to explicitly authorize the existing cybersecurity center within the Department of Homeland Security, so that the Center can continue its important work in serving as a federal civilian information sharing center for cybersecurity. The bill would also codify several other existing Center responsibilities, including authorizing the Center to: (1) provide shared situational awareness to enable quick and coordinated operational actions across the Federal Government; (2) share cybersecurity information and analysis by and among Federal, state, and local government entities and private sector entities; (3) coordinate cybersecurity information sharing throughout the Federal Government; (4) conduct analysis of cybersecurity risks and incidents; (5) provide incident response and technical assistance to federal and non-federal entities; and (6) recommend security and resilience measures to enhance cybersecurity. The bill would continue to

---

[12] *Id.*

[13] Department of Homeland Security, ICS–CERT, Year in Review (2013), page 16, https://ics-cert.us-cert.gov/sites/default/files/documents/Year_In_Review_FY2013_Final.pdf (last viewed July 17, 2014).

[14] Department of Homeland Security, email correspondence to Homeland Security and Government Affairs Committee Staff (July 22, 2014) (on file with Committee).

[15] *Id.*

[16] *Id.*

[17] *Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure*, Hearing before the U.S. Senate Committee on Homeland Security and Governmental Affairs, Testimony of Doug Johnson, On behalf of the Financial Services Sector Coordinating Council (Mar. 26, 2014).

[18] *See* generally, 6 U.S.C. § 121; 6 U.S.C. § 124a; 6 U.S.C. § 143. *See* also 44 U.S.C. § 3546.

allow personnel from Federal agencies, state and local governments, and the private sector to serve at the Center at the discretion of the Under Secretary of the National Protection and Programs Directorate.

III. Legislative History

Chairman Carper and Ranking Member Coburn introduced S. 2519 on June 24, 2014. The bill was referred to the Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 2519 at a business meeting on June 25, 2014. Senator Johnson offered one amendment, clarifying that S. 2519 does not grant the Secretary of Homeland Security any new authority to promulgate regulations or set standards relating to the cybersecurity of private sector critical infrastructure.

The Committee adopted the amendment and then ordered the bill, as amended, reported favorably, both by voice vote. Senators present for both the vote on the amendment and the vote on the bill were Senators Carper, Levin, Pryor, Landrieu, McCaskill, Tester, Heitkamp, Coburn, McCain, Johnson, and Portman. Senators Levin and Tester asked to be recorded as voting no on the amendment.

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

Section 1. Short title.

The short title of the bill is the "National Cybersecurity and Communications Integration Center Act of 2014".

Section 2. National Cybersecurity and Communications Integration Center

Subsection 2(a) of S. 2519 would amend Subtitle A of title II of the Homeland Security Act of 2002 (P.L. 107–296) to add new section—"210G. *Operations Center*."

Subsection 210G(a) of the Homeland Security Act would establish an operations center within the Department of Homeland Security, which may carry out the responsibilities of the Under Secretary appointed under section 103(a)(1)(H) of the Homeland Security Act of 2002 (P.L. 107–296) responsible for security and resilience (currently named the Under Secretary for the National Protection and Programs Directorate). The responsibilities of the operations center would include: serving as a Federal civilian information sharing hub for cybersecurity; providing shared situational awareness to enable real-time operations; sharing cybersecurity threat, vulnerability, impact and incident information and analysis by and among Federal, State, and local government entities and private sectors; coordinating cybersecurity information sharing throughout the Federal government; conducting analysis of cybersecurity risks and incidents; providing technical assistance to Federal and non-Federal entities, upon request, with respect to threats, attribution, vulnerability mitigation, and incident response and remediation; and providing recommendations on security and resilience.

Subsection (b) of the new section of the Homeland Security Act would direct that the center is to be composed, at the discretion of the Under Secretary responsible for overseeing critical infrastruc-

ture protection and cybersecurity (see subsection (e)), of personnel from Federal agencies, including civilian and law enforcement agencies and the intelligence community, and representatives from state and local governments and other non-Federal entities, including representatives from information sharing and analysis organizations and private sector owners and operators of critical infrastructure.

Subsection (c) of the new section of the Homeland Security Act would require the Secretary to submit an annual report one year after the date of enactment of the S. 2519 and for each of the next three years thereafter. The subsection requires the report to include an analysis of the performance of the operations center in carrying out the functions under subsection (a); information on the composition of the center; and information on the policies and procedures established by the center to safeguard privacy and civil liberties.

Subsection (d) of the new section of the Homeland Security Act would require the Government Accountability Office to report to Congress one year after the date of enactment of S. 2519 on the effectiveness of the operations center.

Subsection (e) of the new section of the Homeland Security Act would make clear that it is within the discretion of the Under Secretary whether to include in the center, or provide information and assistance to, governmental or private entities. It also emphasizes that the fact that one private or governmental entity was included in the center or received information or assistance from it does not entitle any other private or governmental entity to such inclusion, information or assistance.

Subsection 2(b) of S. 2519 would amend the table of contents of the Homeland Security Act to reflect the inclusion in the Act of the new section related to the operations center.

Section 3. Rule of construction

Subsection (a) would provide the term "critical infrastructure" the meaning given under section 2 of the Homeland Security Act of 2002.

Subsection (b) provides that S. 2519 does not grant the Secretary of Homeland Security any new authority to promulgate regulations or set standards relating to the cybersecurity of private sector critical infrastructure. Under this subsection, the Secretary retains pre-existing authority to issue regulations or standards relating to the cybersecurity of private sector critical infrastructure.

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

JULY 25, 2014.

Hon. TOM CARPER,
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. 2519, the National Cybersecurity and Communications Integration Center Act of 2014.

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

Sincerely,

DOUGLAS W. ELMENDORF.

Enclosure.

S. 2519—National Cybersecurity and Communications Integration Center Act of 2014

S. 2519 would codify in statute the existence of the National Cybersecurity and Communications Integration Center (NCCIC) of the Department of Homeland Security (DHS). The NCCIC, which was established in 2009, is located in the National Protection and Programs Directorate of DHS and is funded by appropriations provided to the Infrastructure Protection and Information Security appropriation account. So far in 2014 that account has received approximately $1.2 billion, of which almost $800 million is for cybersecurity programs.

S. 2519 would codify NCCIC's current role in protecting federal civilian agencies in cyberspace, sharing information on cybersecurity threats with DHS partners, and analyzing cybersecurity risks and incidents. CBO estimates that implementing the legislation would not result in a significant cost.

Enacting S. 2519 would not affect direct spending or revenues; therefore, pay-as-you-go procedures do not apply.

S. 2519 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would impose no costs on state, local, or tribal governments.

The CBO staff contact for this estimate is Jason Wheelock. The estimate was approved by Theresa Gullo, 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. 2519 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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) * * *

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

* * * * * * *

TITLE II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

* * * * * * *

Subtitle A—Information and Analysis and Infrastructure Protection; Access to Information

* * * * * * *

SEC. 210G. OPERATIONS CENTER.

(a) FUNCTIONS.—There is in the Department an operations center, which may carry out the responsibilities of the Under Secretary appointed under section 103(a)(1)(H) with respect to security and resilience, including by—

(1) serving as a Federal civilian information sharing interface for cybersecurity;

(2) providing shared situational awareness to enable real-time, integrated, and operational actions across the Federal Government;

(3) sharing cybersecurity threat, vulnerability, impact, and incident information and analysis by and among Federal, State, and local government entities and private sector entities;

(4) coordinating cybersecurity information sharing throughout the Federal Government;

(5) conducting analysis of cybersecurity risks and incidents;

(6) upon request, providing timely technical assistance to Federal and non-Federal entities with respect to cybersecurity threats and attribution, vulnerability mitigation, and incident response and remediation; and

(7) providing recommendations on security and resilience measures to Federal and non-Federal entities.

(b) COMPOSITION.—The operations center shall be composed of—

(1) personnel or other representatives of Federal agencies, including civilian and law enforcement agencies and elements of the intelligence community, as such term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)); and

(2) representatives from State and local governments and other non-Federal entities, including—

(A) representatives from information sharing and analysis organizations; and

(B) private sector owners and operators of critical information systems.

(c) ANNUAL REPORT.—Not later than 1 year after the date of enactment of the National Cybersecurity and Communications Inte-

gration Center Act of 2014, and every year thereafter for 3 years, the Secretary 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 operations center, which shall include—

(1) an analysis of the performance of the operations center in carrying out the functions under subsection (a);

(2) information on the composition of the center, including—

(A) the number of representatives from non-Federal entities that are participating in the operations center, including the number of representatives from States, nonprofit organizations, and private sector entities, respectively; and

(B) the number of requests from non-Federal entities to participate in the operations center and the response to such requests, including—

(i) the average length of time to fulfill such identified requests by the Federal agency responsible for fulfilling such requests; and

(ii) a description of any obstacles or challenges to fulfilling such requests; and

(3) the policies and procedures established by the operations center to safeguard privacy and civil liberties.

(d) GAO REPORT.—Not later than 1 year after the date of enactment of the National Cybersecurity and Communications Integration Center Act of 2014, the Comptroller General of the United States 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 effectiveness of the operations center.

(e) NO RIGHT OR BENEFIT.—The provision of assistance or information to, and inclusion in the operations center of, governmental or private entities under this section shall be at the discretion of the Under Secretary appointed under section 103(a)(1)(H). The provision of certain assistance or information to, or inclusion in the operations 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.

* * * * * * *

○