114TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
114–363

STATE AND LOCAL CYBER PROTECTION ACT OF 2015

DECEMBER 3, 2015.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. MCCAUL, from the Committee on Homeland Security, submitted the following

R E P O R T

[To accompany H.R. 3869]

The Committee on Homeland Security, to whom was referred the bill (H.R. 3869) to amend the Homeland Security Act of 2002 to require State and local coordination on cybersecurity with the national cybersecurity and communications integration center, and for other purposes, having considered the same, reports favorably thereon without amendment and recommends that the bill do pass.

CONTENTS

PURPOSE AND SUMMARY

The purpose of H.R. 3869 is to amend the Homeland Security Act of 2002 to assist State and local coordination on cybersecurity with

the national cybersecurity and communications integration center, and for other purposes.The State and Local Cyber Protection Act of 2015 would codify ongoing efforts by instructing the National Cybersecurity and Communications Integration Center (NCCIC) at the Department of Homeland Security (DHS) to coordinate with State and local governments and to, upon request, provide assistance to secure their information systems. The legislation is intended to codify DHS' ongoing coordination effort to give assurances to State and local governments that DHS stands ready to partner with them to protect their networks through existing programs.

The NCCIC would, to the extent practicable, assist in the identification of cyber vulnerabilities and related protections for State and local information security systems, develop a web portal to communicate available tools for State and locals to utilize, provide voluntary technical training for State and local cybersecurity analysts, provide assistance in implementing cybersecurity tools, provide privacy and civil liberties training, and inform State and locals about cybersecurity best practices. The bill would further direct the NCCIC to submit information on the effectiveness of their activities with State and locals to Congress two years after enactment.

BACKGROUND AND NEED FOR LEGISLATION

Cybersecurity remains one of the most significant challenges facing the nation. State and Local governments host a wide range of sensitive citizen and critical infrastructure data that make them especially attractive targets for cyber attacks. In an October 2015 survey sponsored by Hewlett Packard, 71 percent of information technology (IT) and IT security practitioners in State, Local, Tribal and Territorial (SLTT) government identified that their current cybersecurity practices are not clearly defined and that only 19 percent of these SLTT IT practitioners rated their ability in preventing a cyber-attack highly. In November of 2010 in Gregg County, Texas, hackers, reportedly from Russia, managed to steal $200,000 in electronic fund transfers intended for delivery to schools and cities within the county[1]. In January of 2015, pro-ISIS hackers took over a government website of a County government in Virginia for the purpose of spreading propaganda[2].

DHS has an important role to play in coordinating with State and locals to help them protect their information systems. For many State and local governments, DHS is the primary federal government point of contact for assisting with cybersecurity and recovering from a cyber incident and seeking information to bolster their current defenses. DHS presently offers such assistance and collaborates heavily with state and local stakeholders in its cybersecurity activities through the Multi State Information Sharing Analysis Center, the C-Cubed Voluntary Critical Infrastructure Program, the Cyber Resilience Review, the Enhanced Cybersecurity Services Program, the Continuous Diagnostics and Mitigation Program, the National Cyber Awareness System, the Cybersecurity Evaluation Tool (CSET) and the On-Site Cybersecurity Consulting.

---

[1] *http://www.news-journal.com/news/2010/dec/06/cyber-thieves-hit-gregg-county-for-200k/*.

[2] *http://www.newsmax.com/Newsfront/isis-hacker-government-website/2015/01/17/id/619210/*.

HEARINGS

No hearings were held on H.R. 2869, however, the Committee held the following oversight hearing:

On June 24, 2015, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "DHS' Efforts to Secure .Gov." The Subcommittee received testimony from Dr. Andy Ozment, Assistant Secretary, Office of Cybersecurity and Communications, National Protections and Programs Directorate, U.S. Department of Homeland Security; Mr. Gregory C. Wilshusen, Director, Information Security Issues, Government Accountability Office; and Dr. Daniel M. Gerstein, The RAND Corporation.

COMMITTEE CONSIDERATION

The Committee met on November 4, 2015, to consider H.R. 3869, and ordered the measure to be reported to the House with a favorable recommendation, as amended, by voice vote.

COMMITTEE VOTES

Clause 3(b) of Rule XIII of the Rules of the House of Representatives requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

No recorded votes were requested during consideration of H.R. 3869.

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of Rule XIII of the Rules of the House of Representatives, the Committee has held oversight hearings and made findings that are reflected in this report.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of Rule XIII of the Rules of the House of Representatives, the Committee finds that H.R. 3869, the State and Local Cyber Protection Act of 2015, would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

Pursuant to clause 3(c)(3) of Rule XIII of the Rules of the House of Representatives, a cost estimate provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974 was not made available to the Committee in time for the filing of this report. The Chairman of the Committee shall cause such estimate to be printed in the *Congressional Record* upon its receipt by the Committee.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of Rule XIII of the Rules of the House of Representatives, H.R. 3869 contains the following general performance goals and objectives, including outcome related goals and objectives authorized.

H.R. 3869 provides that, not later than 2 years after the date of enactment of this Act, the national cybersecurity and communications integration center of the Department of Homeland Security shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate information on the activities and effectiveness of such activities and will include feedback from State and local governments in this information.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of Rule XIII, the Committee finds that H.R. 3869 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

CONGRESSIONAL EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

In compliance with Rule XXI of the Rules of the House of Representatives, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(e), 9(f), or 9(g) of the Rule XXI.

FEDERAL MANDATES STATEMENT

An estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act was not made available to the Committee in time for the filing of this report. The Chairman of the Committee shall cause such estimate to be printed in the *Congressional Record* upon its receipt by the Committee.

PREEMPTION CLARIFICATION

In compliance with section 423 of the Congressional Budget Act of 1974, requiring the report of any Committee on a bill or joint resolution to include a statement on the extent to which the bill or joint resolution is intended to preempt State, local, or Tribal law, the Committee finds that H.R. 3869 does not preempt any State, local, or Tribal law.

DISCLOSURE OF DIRECTED RULE MAKINGS

The Committee estimates that H.R. 3869 would require no directed rule makings.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short Title.

This section provides that this bill may be cited as the "State and Local Cyber Protection Act of 2015".

Sec. 2. State and Local Coordination on Cybersecurity with the National Cybersecurity and Communications Integration Center.

Subsection (a).

This subsection amends the second section 226 of the Homeland Security Act (HSA) by adding the following:

"Subsection (g) STATE AND LOCAL COORDINATION ON CYBERSECURITY.

The National Cybersecurity and Communications Integration Center (Center) shall, to the extent practicable, offer assistance, tools, and training to State and local governments to address cybersecurity risks and incidents.

This subsection instructs the Center to offer assistance, upon request, to State and Local governments to secure information systems through the identification of cybersecurity risks and relevant protective security tools and the deployment of technology to continuously diagnose and mitigate against cyber threats and vulnerabilities. This subsection instructs the Center to provide a web portal developed in consultation with State and local governments. This subsection also instructs the Center to coordinate nationwide efforts, working with national associations, to secure information systems at the State and local level. One potential mechanism for doing so would be participation and coordination in national meetings that are already in place such as current meetings coordinated by the National Governors Association, the National Association of State Chief Information Officers and other relevant groups.

This subsection instructs the Center to, upon request, provide to State and locals technical cybersecurity training to relevant analysts such as the cyber analysis training course held at Argonne National Laboratory which includes in its target audience analysts supporting State Chief Information Officers and/or Chief Information Security Officers. This subsection also instructs the Center, in coordination with the Chief Privacy Officer and the Chief Civil Rights and Civil Liberties Officer of the Department, to provide privacy and civil liberties training. The subsection also instructs the Center to provide operational and technical assistance for implementing tools, products, resources, policies, guidelines, and procedures for information security. The Center is also instructed to compile and analyze data on State and local information security, and develop and conduct targeted operational evaluations for State and local governments. The Committee believes this legislation reinforces the support and assistance DHS is already providing for State and local governments through existing funded programs.

This subsection also instructs the Center to assist State and locals to develop procedures for coordinating vulnerability disclosures using current standards. It informs State and local govern-

ments on the tools, products, resources, policies, guidelines, and procedures on information security best practices.

Subsection (b) Congressional Oversight.

This subsection requires the Center to submit to the U.S. House of Representatives Committee on Homeland Security and U.S. Senate Committee on Homeland Security and Governmental Affairs two years after the enactment of this bill information on the activities and effectiveness of their coordination efforts with State and local governments. The Center is required to seek feedback from State and local governments and incorporate such feedback into this submitted information.

The Committee intends for this legislation to instruct the Center to execute and provide cybersecurity assistance to State and local governments including by assisting governors and other appointed and elected SLTT government officials with identifying cybersecurity initiatives and partnership opportunities with Federal agencies and State and local associations to help protect their citizens online. The Committee underscores this point by noting that the bill provides no new funding and, as such, is not intended to place new unfunded mandates on DHS. Instead, it seeks to codify the NCCIC to manage existing efforts and to strengthen partnerships with State and local governments.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (new matter is printed in italics 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 C—Information Security

* * * * * * *

SEC. 226. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

(a) DEFINITIONS.—In this section—

(1) the term "cybersecurity risk" means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of information or information systems, including such related consequences caused by an act of terrorism;

(2) the term "incident" means an occurrence that—

(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system; or

(B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies;

(3) the term "information sharing and analysis organization" has the meaning given that term in section 212(5); and

(4) the term "information system" has the meaning given that term in section 3502(8) of title 44, United States Code.

(b) CENTER.—There is in the Department a national cybersecurity and communications integration center (referred to in this section as the "Center") to carry out certain responsibilities of the Under Secretary appointed under section 103(a)(1)(H).

(c) FUNCTIONS.—The cybersecurity functions of the Center shall include—

(1) being a Federal civilian interface for the multi-directional and cross-sector sharing of information related to cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities;

(2) providing shared situational awareness to enable real-time, integrated, and operational actions across the Federal Government and non-Federal entities to address cybersecurity risks and incidents to Federal and non-Federal entities;

(3) coordinating the sharing of information related to cybersecurity risks and incidents across the Federal Government;

(4) facilitating cross-sector coordination to address cybersecurity risks and incidents, including cybersecurity risks and incidents that may be related or could have consequential impacts across multiple sectors;

(5)(A) conducting integration and analysis, including cross-sector integration and analysis, of cybersecurity risks and incidents; and

(B) sharing the analysis conducted under subparagraph (A) with Federal and non-Federal entities;

(6) upon request, providing timely technical assistance, risk management support, and incident response capabilities to Federal and non-Federal entities with respect to cybersecurity risks and incidents, which may include attribution, mitigation, and remediation; and

(7) providing information and recommendations on security and resilience measures to Federal and non-Federal entities, including information and recommendations to—

(A) facilitate information security; and

(B) strengthen information systems against cybersecurity risks and incidents.

(d) COMPOSITION.—

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

(A) appropriate representatives of Federal entities, such as—

(i) sector-specific agencies;

(ii) civilian and law enforcement agencies; and

(iii) elements of the intelligence community, as that term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4));

(B) appropriate representatives of non-Federal entities, such as—

(i) State and local governments;

(ii) information sharing and analysis organizations; and

(iii) owners and operators of critical information systems;

(C) components within the Center that carry out cybersecurity and communications activities;

(D) a designated Federal official for operational coordination with and across each sector; and

(E) other appropriate representatives or entities, as determined by the Secretary.

(2) INCIDENTS.—In the event of an incident, during exigent circumstances the Secretary may grant a Federal or non-Federal entity immediate temporary access to the Center.

(e) PRINCIPLES.—In carrying out the functions under subsection (c), the Center shall ensure—

(1) to the extent practicable, that—

(A) timely, actionable, and relevant information related to cybersecurity risks, incidents, and analysis is shared;

(B) when appropriate, information related to cybersecurity risks, incidents, and analysis is integrated with other relevant information and tailored to the specific characteristics of a sector;

(C) activities are prioritized and conducted based on the level of risk;

(D) industry sector-specific, academic, and national laboratory expertise is sought and receives appropriate consideration;

(E) continuous, collaborative, and inclusive coordination occurs—

(i) across sectors; and

(ii) with—

(I) sector coordinating councils;

(II) information sharing and analysis organizations; and

(III) other appropriate non-Federal partners;

(F) as appropriate, the Center works to develop and use mechanisms for sharing information related to cybersecurity risks and incidents that are technology-neutral, interoperable, real-time, cost-effective, and resilient; and

(G) the Center works with other agencies to reduce unnecessarily duplicative sharing of information related to cybersecurity risks and incidents;

(2) that information related to cybersecurity risks and incidents is appropriately safeguarded against unauthorized access; and

(3) that activities conducted by the Center comply with all policies, regulations, and laws that protect the privacy and civil liberties of United States persons.

(f) NO RIGHT OR BENEFIT.—

(1) IN GENERAL.—The provision of assistance or information to, and inclusion in 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 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) STATE AND LOCAL COORDINATION ON CYBERSECURITY.—

(1) IN GENERAL.—The Center shall, to the extent practicable—

(A) assist State and local governments, upon request, in identifying information system vulnerabilities;

(B) assist State and local governments, upon request, in identifying information security protections commensurate with cybersecurity risks and the magnitude of the potential harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

(i) information collected or maintained by or on behalf of a State or local government; or

(ii) information systems used or operated by an agency or by a contractor of a State or local government or other organization on behalf of a State or local government;

(C) in consultation with State and local governments, provide and periodically update via a web portal tools, products, resources, policies, guidelines, and procedures related to information security;

(D) work with senior State and local government officials, including State and local Chief Information Officers, through national associations to coordinate a nationwide effort to ensure effective implementation of tools, products, resources, policies, guidelines, and procedures related to information security to secure and ensure the resiliency of State and local information systems;

(E) provide, upon request, operational and technical cybersecurity training to State and local government and fusion center analysts and operators to address cybersecurity risks or incidents;

(F) provide, in coordination with the Chief Privacy Officer and the Chief Civil Rights and Civil Liberties Officer of the Department, privacy and civil liberties training to State and local governments related to cybersecurity;

(G) provide, upon request, operational and technical assistance to State and local governments to implement tools, products, resources, policies, guidelines, and procedures on information security by—

(i) deploying technology to assist such State or local government to continuously diagnose and mitigate against cyber threats and vulnerabilities, with or without reimbursement;

(ii) compiling and analyzing data on State and local information security; and

(iii) developing and conducting targeted operational evaluations, including threat and vulnerability assess-

ments, on the information systems of State and local governments;

(H) assist State and local governments to develop policies and procedures for coordinating vulnerability disclosures, to the extent practicable, consistent with international and national standards in the information technology industry, including standards developed by the National Institute of Standards and Technology; and

(I) ensure that State and local governments, as appropriate, are made aware of the tools, products, resources, policies, guidelines, and procedures on information security developed by the Department and other appropriate Federal departments and agencies for ensuring the security and resiliency of Federal civilian information systems.

(2) TRAINING.—Privacy and civil liberties training provided pursuant to subparagraph (F) of paragraph (1) shall include processes, methods, and information that—

(A) are consistent with the Department's Fair Information Practice Principles developed pursuant to section 552a of title 5, United States Code (commonly referred to as the "Privacy Act of 1974" or the "Privacy Act");

(B) reasonably limit, to the greatest extent practicable, the receipt, retention, use, and disclosure of information related to cybersecurity risks and incidents associated with specific persons that is not necessary, for cybersecurity purposes, to protect an information system or network of information systems from cybersecurity risks or to mitigate cybersecurity risks and incidents in a timely manner;

(C) minimize any impact on privacy and civil liberties;

(D) provide data integrity through the prompt removal and destruction of obsolete or erroneous names and personal information that is unrelated to the cybersecurity risk or incident information shared and retained by the Center in accordance with this section;

(E) include requirements to safeguard cyber threat indicators and defensive measures retained by the Center, including information that is proprietary or business-sensitive that may be used to identify specific persons from unauthorized access or acquisition;

(F) protect the confidentiality of cyber threat indicators and defensive measures associated with specific persons to the greatest extent practicable; and

(G) ensure all relevant constitutional, legal, and privacy protections are observed.

* * * * * * *

○