114TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
114–565

NATIONAL CYBERSECURITY PREPAREDNESS CONSORTIUM ACT OF 2016

MAY 13, 2016.—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. 4743]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 4743) to authorize the Secretary of Homeland Security to establish a National Cybersecurity Preparedness Consortium, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "National Cybersecurity Preparedness Consortium Act of 2016".

SEC. 2. NATIONAL CYBERSECURITY PREPAREDNESS CONSORTIUM.

(a) IN GENERAL.—The Secretary of Homeland Security may work with a consortium, including the National Cybersecurity Preparedness Consortium, to support efforts to address cybersecurity risks and incidents (as such terms are defined in section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148)), including threats of terrorism and acts of terrorism.

(b) ASSISTANCE TO THE NCCIC.—The Secretary of Homeland Security may work with a consortium to assist the national cybersecurity and communications integration center of the Department of Homeland Security (established pursuant to section 227 of the Homeland Security Act of 2002) to—

(1) provide training to State and local first responders and officials specifically for preparing for and responding to cybersecurity risks and incidents, including threats of terrorism and acts of terrorism, in accordance with current law;

(2) develop and update a curriculum utilizing existing programs and models in accordance with such section 227, for State and local first responders and officials, related to cybersecurity risks and incidents, including threats of terrorism and acts of terrorism;

(3) provide technical assistance services to build and sustain capabilities in support of preparedness for and response to cybersecurity risks and incidents, including threats of terrorism and acts of terrorism, in accordance with such section 227;

(4) conduct cross-sector cybersecurity training and simulation exercises for entities, including State and local governments, critical infrastructure owners and operators, and private industry, to encourage community-wide coordination in defending against and responding to cybersecurity risks and incidents, including threats of terrorism and acts of terrorism, in accordance with subsection (c) of section 228 of the Homeland Security Act of 2002 (6 U.S.C. 149);

(5) help States and communities develop cybersecurity information sharing programs, in accordance with section 227 of the Homeland Security Act of 2002, for the dissemination of homeland security information related to cybersecurity risks and incidents, including threats of terrorism and acts of terrorism; and

(6) help incorporate cybersecurity risk and incident prevention and response (including related to threats of terrorism and acts of terrorism) into existing State and local emergency plans, including continuity of operations plans.

(c) PROHIBITION ON DUPLICATION.—In carrying out the functions under subsection (b), the Secretary of Homeland Security shall, to the greatest extent practicable, seek to prevent unnecessary duplication of existing programs or efforts of the Department of Homeland Security.

(d) CONSIDERATIONS REGARDING SELECTION OF A CONSORTIUM.—In selecting a consortium with which to work under this Act, the Secretary of Homeland Security shall take into consideration the following:

(1) Any prior experience conducting cybersecurity training and exercises for State and local entities.

(2) Geographic diversity of the members of any such consortium so as to cover different regions across the United States.

(e) METRICS.—If the Secretary of Homeland Security works with a consortium pursuant to subsection (a), the Secretary shall measure the effectiveness of the activities undertaken by such consortium under this Act.

(f) OUTREACH.—The Secretary of Homeland Security shall conduct outreach to universities and colleges, including historically Black colleges and universities, Hispanic-serving institutions, Tribal Colleges and Universities, and other minority-serving institutions, regarding opportunities to support efforts to address cybersecurity risks and incidents, including threats of terrorism and acts of terrorism, by working with the Secretary pursuant to subsection (a).

(g) TERMINATION.—The authority to carry out this Act shall terminate on the date that is five years after the date of the enactment of this Act.

(h) CONSORTIUM DEFINED.—In this Act, the term "consortium" means a group primarily composed of non-profit entities, including academic institutions, that develop, update, and deliver cybersecurity training in support of homeland security.

PURPOSE AND SUMMARY

H.R. 4743 allows the U.S. Department of Homeland Security (DHS) to work with a consortium, including the National Cybersecurity Preparedness Consortium, to support efforts to address cybersecurity risks and incidents. DHS may also engage a consortium to assist the National Cybersecurity and Communications Integration Center (NCCIC) in providing training to State and local first responders in preparing for and responding to cybersecurity risks and incidents. The NCCIC is the central location where cyber operations are conducted at DHS.

BACKGROUND AND NEED FOR LEGISLATION

The Department of Homeland Security and, specifically, the NCCIC are responsible for carrying out significant aspects of the Federal Government's cybersecurity mission. In December 2015, the Cybersecurity Act was signed into law authorizing DHS to share cyber threat indicators and defensive measures with the private sector. Also, in December 2015, the House passed H.R. 3869, the State and Local Cyber Protection Act of 2015, that instructed the NCCIC to assist State and local entities to secure their information systems.

This bill would allow DHS to work with, for example, the National Cybersecurity Preparedness Consortium (NCPC or "the Consortium") which currently provides State and local communities with tools to prevent, detect, respond to, and recover from cyber attacks as they would any other disaster or emergency situation. The Consortium evaluates communities' cybersecurity posture and provides them with a roadmap to correct deficiencies in the security of their information systems. Based out of the University of Texas San Antonio's Center for Infrastructure Assurance and Security, the NCPC has members located throughout the country, including the Criminal Justice Institute at the University of Arkansas, the University of Memphis Center for Information Assurance, the Norwich University Applied Research Institutes, and the Texas A&M Engineering Extension Service.

HEARINGS

On April 7, 2016, the Subcommittee held a field hearing in Sherman, Texas, entitled "Cyber Preparedness and Response at the Local Level." The Subcommittee received testimony from Mr. Alphonse G. Davis, Deputy Director/Chief Operations Officer, Texas A&M Engineering Extension Service; Mr. Sam Greif, Chief, Plano Fire-Rescue Department, Plano, Texas, *testifying on behalf of the International Association of Fire Chiefs*; Mr. Richard F. Wilson, Lieutenant, Dallas Police Department, Dallas, Texas; and Mr. Don Waddle, Detective (Ret.), Greenville Police Department, Greenville, Texas.

COMMITTEE CONSIDERATION

The Committee met on April 28, 2016, to consider H.R. 4743, and ordered the measure to be reported to the House with a favorable recommendation, as amended, by unanimous consent. The Committee took the following actions:

The following amendments were offered:

An Amendment in the Nature of a Substitute offered by RICHMOND (#1); was AGREED TO, as amended, by unanimous consent.

An amendment by MS. JACKSON LEE to the Amendment in the Nature of a Substitute (#1A); was AGREED TO by unanimous consent.

In section 2(a), insert a comma after "Consortium".

In section 2, insert after subsection (d) a new subsection (and redesignate subsequent subsections accordingly) entitled "(d) Metrics."

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. 4743.

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. 4743, the National Cybersecurity Preparedness Consortium Act of 2016, would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, May 13, 2016.

Hon. MICHAEL MCCAUL,
Chairman, Committee on Homeland Security,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 4743, the National Cybersecurity Preparedness Consortium Act of 2016.

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.

Enclosure.

H.R. 4743—National Cybersecurity Preparedness Consortium Act of 2016

H.R. 4743 would authorize the Department of Homeland Security (DHS) to work with a consortium, including the National Cybersecurity Preparedness Consortium (NCPC), to assist state and local governments to prepare for, and respond to, cybersecurity risks and incidents over the five-year period immediately following the bill's enactment. Since 2014, NCPC has received about $6 million in grant funding from the Federal Emergency Management Agency to deliver cybersecurity training, exercises, and technical assistance to state and local governments. If implemented, CBO expects that DHS's level of involvement under H.R. 4743 would remain unchanged and would consist primarily of reviewing and approving NCPC's future applications for grant funding. Therefore, CBO estimates that to maintain a similar level of support as is currently provided by the NCPC to state and local governments, it would cost $15 million (average of $3 million per year in new grant funding) over the 2017–2021 period, assuming appropriation of the estimated amounts.

Enacting H.R. 4743 would not affect direct spending or revenues; therefore, pay-as-you-go procedures do not apply.

CBO estimates that enacting H.R. 4743 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2027.

H.R. 4743 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and could benefit state and local law enforcement agencies by authorizing federal technical assistance and training for cybersecurity activities. Any costs incurred by those agencies would result from participation in voluntary federal programs.

The CBO staff contact for this estimate is William Ma. The estimate was approved by H. Samuel Papenfuss, Deputy Assistant Director for Budget Analysis.

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. 4743 contains the following general performance goals and objectives, including outcome related goals and objectives authorized.

This legislation allows the Secretary to work with any consortium, including the National Cybersecurity Preparedness Consortium, to support efforts to address cybersecurity risks and incidents. It also requires the Secretary of Homeland Security to measure the effectiveness of the activities undertaken by consortia under this Act.

Duplicative Federal Programs

Pursuant to clause 3(c) of Rule XIII, the Committee finds that H.R. 4743 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 Rule XXI.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

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. 4743 does not preempt any State, local, or Tribal law.

DISCLOSURE OF DIRECTED RULE MAKINGS

The Committee estimates that H.R. 4743 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 "National Cybersecurity Preparedness Consortium Act of 2016".

Sec. 2. National Cybersecurity Preparedness Consortium.

This section provides the Secretary of Homeland Security with authority to work with any consortium, including the National Cybersecurity Preparedness Consortium, to support efforts to address cybersecurity risks and incidents. These efforts may include: Assisting the National Cybersecurity and Communications Integration Center (NCCIC) to: 1) Provide training to State and local first responders for preparing for and responding to cybersecurity risks and incidents; 2) develop and update curriculum for State and local first responders and officials, related to cybersecurity risks and incidents; 3) provide technical assistance services to build and sustain capabilities in support of preparedness for and response to cybersecurity risks and incidents; 4) conduct cross-sector cybersecu-

rity training and simulation exercises for entities to encourage community-wide coordination in defending against and responding to cybersecurity risks and incidents; 5) help States and communities develop cybersecurity information sharing programs for the dissemination of homeland security information related to cybersecurity risks and incidents; and 6) help incorporate cybersecurity risk and incident prevention and response into existing State and local emergency plans.

This section requires the Secretary to prevent unnecessary duplication of existing DHS programs or efforts.

This section requires the Secretary to take 1) Prior experience conducting cybersecurity training and exercises for State and local entities, and 2) geographic diversity of the members of the consortium, into consideration in selecting a consortium.

This section requires the Secretary to measure the effectiveness of the activities undertaken with any consortium.

This section requires the Secretary to conduct outreach to colleges and universities, including historically Black colleges and universities, Hispanic-serving institutions, Tribal Colleges and Universities, and other minority-serving institutions, regarding opportunities to support efforts to address cybersecurity risks and incidents.

This section terminates the authority provided in this Act five years after the date of enactment.

This section defines the term "consortium" as a group primarily composed of non-profit entities, including academic institutions, that develop, update, and deliver cybersecurity training in support of homeland security.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

As reported, H.R. 4743 makes no changes to existing law.

○