115TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
115–910

ADVANCING CYBERSECURITY DIAGNOSTICS AND MITIGATION ACT

AUGUST 28, 2018.—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. 6443]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 6443) to amend the Homeland Security Act of 2002 to authorize the Secretary of Homeland Security to establish a continuous diagnostics and mitigation program at the Department of Homeland Security, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

79–006

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 "Advancing Cybersecurity Diagnostics and Mitigation Act".

SEC. 2. ESTABLISHMENT OF CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM IN DEPARTMENT OF HOMELAND SECURITY.

(a) IN GENERAL.—Section 230 of the Homeland Security Act of 2002 (6 U.S.C. 151) is amended by adding at the end the following new subsection:

"(g) CONTINUOUS DIAGNOSTICS AND MITIGATION.—

"(1) PROGRAM.—

"(A) IN GENERAL.—The Secretary shall deploy, operate, and maintain a continuous diagnostics and mitigation program. Under such program, the Secretary shall—

"(i) develop and provide the capability to collect, analyze, and visualize information relating to security data and cybersecurity risks;

"(ii) make program capabilities available for use, with or without reimbursement;

"(iii) employ shared services, collective purchasing, blanket purchase agreements, and any other economic or procurement models the Secretary determines appropriate to maximize the costs savings associated with implementing an information system;

"(iv) assist entities in setting information security priorities and managing cybersecurity risks; and

"(v) develop policies and procedures for reporting systemic cybersecurity risks and potential incidents based upon data collected under such program.

"(B) REGULAR IMPROVEMENT.—The Secretary shall regularly deploy new technologies and modify existing technologies to the continuous diagnostics and mitigation program required under subparagraph (A), as appropriate, to improve the program.

"(2) ACTIVITIES.—In carrying out the continuous diagnostics and mitigation program under paragraph (1), the Secretary shall ensure, to the extent practicable, that—

"(A) timely, actionable, and relevant cybersecurity risk information, assessments, and analysis are provided in real time;

"(B) share the analysis and products developed under such program;

"(C) all information, assessments, analyses, and raw data under such program is made available to the national cybersecurity and communications integration center of the Department; and

"(D) provide regular reports on cybersecurity risks.".

(b) CONTINUOUS DIAGNOSTICS AND MITIGATION STRATEGY.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall develop a comprehensive continuous diagnostics and mitigation strategy to carry out the continuous diagnostics and mitigation program required under subsection (g) of section 230 of such Act, as added by subsection (a).

(2) SCOPE.—The strategy required under paragraph (1) shall include the following:

(A) A description of the continuous diagnostics and mitigation program, including efforts by the Secretary of Homeland Security to assist with the deployment of program tools, capabilities, and services, from the inception of the program referred to in paragraph (1) to the date of the enactment of this Act.

(B) A description of the coordination required to deploy, install, and maintain the tools, capabilities, and services that the Secretary of Homeland Security determines to be necessary to satisfy the requirements of such program.

(C) A description of any obstacles facing the deployment, installation, and maintenance of tools, capabilities, and services under such program.

(D) Recommendations and guidelines to help maintain and continuously upgrade tools, capabilities, and services provided under such program.

(E) Recommendations for using the data collected by such program for creating a common framework for data analytics, visualization of enterprise-wide risks, and real-time reporting.

(F) Recommendations for future efforts and activities, including for the rollout of new tools, capabilities and services, proposed timelines for deliv-

ery, and whether to continue the use of phased rollout plans, related to securing networks, devices, data, and information technology assets through the use of such program.

(3) FORM.—The strategy required under subparagraph (A) shall be submitted in an unclassified form, but may contain a classified annex.

(c) REPORT.—Not later than 90 days after the development of the strategy required under subsection (b), the Secretary of Homeland Security shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representative a report on cybersecurity risk posture based on the data collected through the continuous diagnostics and mitigation program under subsection (g) of section 230 of the Homeland Security Act of 2002, as added by subsection (a).

PURPOSE AND SUMMARY

H.R. 6443, the "Advancing Cybersecurity Diagnostics and Mitigation Act," codifies and defines the activities of the continuous diagnostics and mitigation (CDM) program at the Department of Homeland Security (DHS). The bill requires the Secretary of Homeland Security to deploy, operate, and maintain the CDM program, developing and providing capabilities to collect, analyze, and visualize information related to security data and cybersecurity risk. H.R. 6443 requires the Secretary to make these capabilities available, with or without reimbursement. The Secretary is also required to develop policies and procedures for reporting systemic cybersecurity risks and potential incidents based upon data collected under CDM.

The bill requires the Secretary to regularly deploy new CDM technologies and modify existing CDM capabilities to continuously improve the program. H.R. 6443 also requires the Secretary to ensure timely, actionable, and relevant cybersecurity risk information, assessments, and analysis are provided in real time while ensuring all raw data is made available to the National Cybersecurity and Communications Integration Center (NCCIC). Additionally, the bill requires DHS to develop a strategy to ensure the program continues to evolve and adjust to the changing cyber threat landscape and requires the strategy to be shared with Congress.

BACKGROUND AND NEED FOR LEGISLATION

DHS's National Protection and Programs Directorate (NPPD) is currently in the process of implementing a four-phase rollout of CDM capabilities at participating federal agencies. The CDM program office has been working with federal civilian agencies and departments, including the 24 Chief Financial Officer (CFO) Act agencies to deploy CDM functionality since 2013. To provide near-real time effective continuous monitoring and mitigation, agencies and DHS will not only need to implement all four phases and deploy CDM dashboards, but also evolve cybersecurity tools to address the growing threats the federal enterprise faces.

CDM tools and data provide individual agencies improved visibility and understanding of their systems and networks. The CDM program also provides DHS with broad situational awareness and places DHS in a strong position to leverage individual agency data to identify, respond to, and mitigate cybersecurity vulnerabilities and threats. In this way, DHS can utilize CDM to consolidate some of the federal government's cybersecurity responsibilities, allowing agencies to focus on the specific and unique cybersecurity risks their agency is facing.

H.R. 6443 will codify the work of CDM to date, while ensuring DHS continues to update CDM technologies to regularly improve the program and develops a long-term strategy to strengthen the future of the program.

HEARINGS

The Committee did not hold any specific hearing specifically on H.R. 6443. However, the Subcommittee on Cybersecurity and Infrastructure Protection held a joint hearing with the House Oversight and Government Reform, Subcommittee on Information Technology on January 17, 2018 entitled, "CDM, the Future of Federal Cybersecurity" to understand the current state of the CDM program from the perspective of stakeholders. Testimony was heard from Frank Dimina, Area Vice President, Splunk; Dan Carayiannis, Public Sector Director, RSA Archer; Gregg Mossburg, Senior Vice President for Strategic Operations, CGI Federal; and A.R. "Trey" Hodgkins, III, Senior Vice President, Public Sector, Information Technology Alliance for Public Sector.

The Subcommittee on Cybersecurity and Infrastructure Protection held a hearing on March 20, 2018 entitled, "CDM: Government Perspectives on Security and Modernization" to explore the development, deployment, and utilization of the CDM program by federal agencies. Testimony was heard from Max Everett, Chief Information Officer, Department of Energy; Scott Blackburn, Executive in Charge, Office of Information and Technology, Department of Veterans Affairs; David Garcia, Chief Information Officer, Office of Personnel Management; and Kevin Cox, Program Manager, Continuous Diagnostics and Mitigation, Office of Cybersecurity and Communications, National Protection and Programs Directorate, Department of Homeland Security.

COMMITTEE CONSIDERATION

The Committee met on July 24, 2018, to consider H.R. 6443, and ordered the measure to be reported to the House with a favorable recommendation, amended by Mr. Langevin. The Committee took the following actions:

The following amendments were offered:

An Amendment by MR. LANGEVIN to the bill (#1); was accepted by unanimous consent.

Consisting of the following amendments:

On page (5) in line (17), insert ", including for the rollout of new tools, capabilities and services, proposed timelines for delivery, and whether to continue the use of phased rollout plans," after "activities"

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. 6443.

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. 6443, the Advancing Cybersecurity Diagnostics and Mitigation Act, 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, August 1, 2018.

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. 6443, the Advancing Cybersecurity Diagnostics and Mitigation Act.

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.

H.R. 6443—Advancing Cybersecurity Diagnostics and Mitigation Act

H.R. 6443 would require the Department of Homeland Security (DHS) to deploy, operate, and maintain a continuous diagnostics and mitigation (CDM) program to assist federal agencies to improve the cybersecurity of their respective networks and systems. Based on information from DHS, the department already makes available to all federal agencies the capabilities required in the bill; thus, the bill would codify in law current activities.

H.R. 6443 also would require DHS, within 180 days of the bill's enactment, to develop and submit to the Congress a strategy to carry out the CDM program. Not later than 90 days after developing that strategy, the bill also would require DHS to submit a report to the Congress on the cybersecurity strength of federal networks and systems based on the data collected through the CDM program. Based on the cost of similar activities, CBO estimates that preparing the strategy and report would cost less than $500,000 over the 2019–2023 period; such spending would be subject to the availability of appropriated amounts.

Enacting H.R. 6443 would not affect direct spending or revenues; therefore, pay-as-you-go procedures do not apply.

CBO estimates that enacting H.R. 6443 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2029.

H.R. 6443 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.

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. 6443 contains the following general performance goals and objectives, including outcome related goals and objectives authorized.

H.R. 6443 requires the Secretary of Homeland Security to provide House and Senate Homeland Security Committees a report on cybersecurity risk posture based on the data collected through the continuous diagnostics and mitigation program under this bill.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 6443 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

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. 6443 does not preempt any State, local, or Tribal law.

DISCLOSURE OF DIRECTED RULE MAKINGS

The Committee estimates that H.R. 6443 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 "Advancing Cybersecurity Diagnostics and Mitigation Act".

Sec. 2. Establishment of Continuous Diagnostics and Mitigation Program in Department of Homeland Security

Section 2(a) amends the Homeland Security Act of 2002 in Section 230 (6 U.S.C. 151), by creating a new subsection (g) entitled "Continuous Diagnostics and Mitigation."

This section requires the Secretary to deploy, operate, and maintain a continuous diagnostics and mitigation (CDM) program that includes the capability to collect, analyze, and visualize security data and cybersecurity risk information. The Committee intends for agencies to make available raw data and information available to DHS to continue to support the efficacy and accuracy of risk assessments based on or in part by the CDM program.

This section requires the Secretary to make the CDM program available to agencies, with or without reimbursement; to leverage collective economic and procurement models to maximize cost savings; to assist in setting information security priorities and managing cybersecurity risk; and to develop policies and procedures on reporting cybersecurity risks and potential incidents.

This section defines the activities of CDM to produce timely, actionable, and relevant cybersecurity risk information, assessments and analysis in real time; to share analysis and products with federal and non-Federal entities; to ensure all information, assessments, analysis and raw data is made available to the National Cybersecurity Integration Center (NCCIC); and to provide regular reports on cybersecurity risks.

Section 2(b) requires the Secretary to develop a comprehensive strategy for the CDM program, consistent with the purpose and activities established in this bill. The strategy must include a description of the current state of the program, how the program is being coordinated, a description of any obstacles to fully establishing the CDM program, recommendations for maintaining CDM capabilities and optimizing the use of CDM data collected, and recommendations for future activities. The strategy must be presented in an unclassified form but may include a classified annex. The Committee intends for the strategy to include recommendations that are applicable to all federal agencies and departments, and departments, and for the strategy to examine whether or not the capabilities of the program should continue to be rolled out in phases or in some

other manner. The Committee intends for the strategy to address the metrics necessary to measure the effectiveness of the CDM program in reducing cybersecurity risks across the federal enterprise

This section requires the Secretary of Homeland Security to produce a report to Congress on cybersecurity risk posture based on the data collected through the CDM program. The Committee intends for the report to address the cybersecurity risk posture of the entire federal enterprise.

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 italic 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. 230. FEDERAL INTRUSION DETECTION AND PREVENTION SYSTEM.

(a) DEFINITIONS.—In this section—

(1) the term "agency" has the meaning given the term in section 3502 of title 44, United States Code;

(2) the term "agency information" means information collected or maintained by or on behalf of an agency;

(3) the term "agency information system" has the meaning given the term in section 228; and

(4) the terms "cybersecurity risk" and "information system" have the meanings given those terms in section 227.

(b) REQUIREMENT.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this section, the Secretary shall deploy, operate, and maintain, to make available for use by any agency, with or without reimbursement—

(A) a capability to detect cybersecurity risks in network traffic transiting or traveling to or from an agency information system; and

(B) a capability to prevent network traffic associated with such cybersecurity risks from transiting or traveling to or from an agency information system or modify such network traffic to remove the cybersecurity risk.

(2) REGULAR IMPROVEMENT.—The Secretary shall regularly deploy new technologies and modify existing technologies to

the intrusion detection and prevention capabilities described in paragraph (1) as appropriate to improve the intrusion detection and prevention capabilities.

(c) ACTIVITIES.—In carrying out subsection (b), the Secretary—

(1) may access, and the head of an agency may disclose to the Secretary or a private entity providing assistance to the Secretary under paragraph (2), information transiting or traveling to or from an agency information system, regardless of the location from which the Secretary or a private entity providing assistance to the Secretary under paragraph (2) accesses such information, notwithstanding any other provision of law that would otherwise restrict or prevent the head of an agency from disclosing such information to the Secretary or a private entity providing assistance to the Secretary under paragraph (2);

(2) may enter into contracts or other agreements with, or otherwise request and obtain the assistance of, private entities to deploy, operate, and maintain technologies in accordance with subsection (b);

(3) may retain, use, and disclose information obtained through the conduct of activities authorized under this section only to protect information and information systems from cybersecurity risks;

(4) shall regularly assess through operational test and evaluation in real world or simulated environments available advanced protective technologies to improve detection and prevention capabilities, including commercial and noncommercial technologies and detection technologies beyond signature-based detection, and acquire, test, and deploy such technologies when appropriate;

(5) shall establish a pilot through which the Secretary may acquire, test, and deploy, as rapidly as possible, technologies described in paragraph (4); and

(6) shall periodically update the privacy impact assessment required under section 208(b) of the E-Government Act of 2002 (44 U.S.C. 3501 note).

(d) PRINCIPLES.—In carrying out subsection (b), the Secretary shall ensure that—

(1) activities carried out under this section are reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

(2) information accessed by the Secretary will be retained no longer than reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

(3) notice has been provided to users of an agency information system concerning access to communications of users of the agency information system for the purpose of protecting agency information and the agency information system; and

(4) the activities are implemented pursuant to policies and procedures governing the operation of the intrusion detection and prevention capabilities.

(e) PRIVATE ENTITIES.—

(1) CONDITIONS.—A private entity described in subsection (c)(2) may not—

(A) disclose any network traffic transiting or traveling to or from an agency information system to any entity other than the Department or the agency that disclosed the information under subsection (c)(1), including personal information of a specific individual or information that identifies a specific individual not directly related to a cybersecurity risk; or

(B) use any network traffic transiting or traveling to or from an agency information system to which the private entity gains access in accordance with this section for any purpose other than to protect agency information and agency information systems against cybersecurity risks or to administer a contract or other agreement entered into pursuant to subsection (c)(2) or as part of another contract with the Secretary.

(2) LIMITATION ON LIABILITY.—No cause of action shall lie in any court against a private entity for assistance provided to the Secretary in accordance with this section and any contract or agreement entered into pursuant to subsection (c)(2).

(3) RULE OF CONSTRUCTION.—Nothing in paragraph (2) shall be construed to authorize an Internet service provider to break a user agreement with a customer without the consent of the customer.

(f) PRIVACY OFFICER REVIEW.—Not later than 1 year after the date of enactment of this section, the Privacy Officer appointed under section 222, in consultation with the Attorney General, shall review the policies and guidelines for the program carried out under this section to ensure that the policies and guidelines are consistent with applicable privacy laws, including those governing the acquisition, interception, retention, use, and disclosure of communications.

(g) CONTINUOUS DIAGNOSTICS AND MITIGATION.—

(1) PROGRAM.—

(A) IN GENERAL.—The Secretary shall deploy, operate, and maintain a continuous diagnostics and mitigation program. Under such program, the Secretary shall—

(i) develop and provide the capability to collect, analyze, and visualize information relating to security data and cybersecurity risks;

(ii) make program capabilities available for use, with or without reimbursement;

(iii) employ shared services, collective purchasing, blanket purchase agreements, and any other economic or procurement models the Secretary determines appropriate to maximize the costs savings associated with implementing an information system;

(iv) assist entities in setting information security priorities and managing cybersecurity risks; and

(v) develop policies and procedures for reporting systemic cybersecurity risks and potential incidents based upon data collected under such program.

(B) REGULAR IMPROVEMENT.—The Secretary shall regularly deploy new technologies and modify existing technologies to the continuous diagnostics and mitigation pro-

gram required under subparagraph (A), as appropriate, to improve the program.

(2) ACTIVITIES.—In carrying out the continuous diagnostics and mitigation program under paragraph (1), the Secretary shall ensure, to the extent practicable, that—

(A) timely, actionable, and relevant cybersecurity risk information, assessments, and analysis are provided in real time;

(B) share the analysis and products developed under such program;

(C) all information, assessments, analyses, and raw data under such program is made available to the national cybersecurity and communications integration center of the Department; and

(D) provide regular reports on cybersecurity risks.

* * * * * * *

○