115TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
115–961

PUBLIC-PRIVATE CYBERSECURITY COOPERATION ACT

SEPTEMBER 25, 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. 6735]

The Committee on Homeland Security, to whom was referred the bill (H.R. 6735) to direct the Secretary of Homeland Security to establish a vulnerability disclosure policy for Department of Homeland Security internet websites, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

	Page
Purpose and Summary	3
Background and Need for Legislation	3
Hearings	4
Committee Consideration	4
Committee Votes	5
Committee Oversight Findings	5
New Budget Authority, Entitlement Authority, and Tax Expenditures	5
Congressional Budget Office Estimate	5
Statement of General Performance Goals and Objectives	5
Duplicative Federal Programs	5
Congressional Earmarks, Limited Tax Benefits, and Limited Tariff Benefits	5
Federal Mandates Statement	6
Preemption Clarification	6
Disclosure of Directed Rule Makings	6
Advisory Committee Statement	6
Applicability to Legislative Branch	6
Section-by-Section Analysis of the Legislation	6
Changes in Existing Law Made by the Bill, as Reported	7

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 "Public-Private Cybersecurity Cooperation Act".

SEC. 2. DEPARTMENT OF HOMELAND SECURITY DISCLOSURE OF SECURITY VULNERABILITIES.

(a) VULNERABILITY DISCLOSURE POLICY.—The Secretary of Homeland Security shall establish a policy applicable to individuals, organizations, and companies that report security vulnerabilities on appropriate information systems of Department of Homeland Security. Such policy shall include each of the following:

(1) The appropriate information systems of the Department that individuals, organizations, and companies may use to discover and report security vulnerabilities on appropriate information systems.

(2) The conditions and criteria under which individuals, organizations, and companies may operate to discover and report security vulnerabilities.

(3) How individuals, organizations, and companies may disclose to the Department security vulnerabilities discovered on appropriate information systems of the Department.

(4) The ways in which the Department may communicate with individuals, organizations, and companies that report security vulnerabilities.

(5) The process the Department shall use for public disclosure of reported security vulnerabilities.

(b) REMEDIATION PROCESS.—The Secretary of Homeland Security shall develop a process for the Department of Homeland Security to address the mitigation or remediation of the security vulnerabilities reported through the policy developed in subsection (a).

(c) CONSULTATION.—In developing the security vulnerability disclosure policy under subsection (a), the Secretary of Homeland Security shall consult with each of the following:

(1) The Attorney General regarding how to ensure that individuals, organizations, and companies that comply with the requirements of the policy developed under subsection (a) are protected from prosecution under section 1030 of title 18, United States Code, civil lawsuits, and similar provisions of law with respect to specific activities authorized under the policy.

(2) The Secretary of Defense and the Administrator of General Services regarding lessons that may be applied from existing vulnerability disclosure policies.

(3) Non-governmental security researchers.

(d) PUBLIC AVAILABILITY.—The Secretary of Homeland Security shall make the policy developed under subsection (a) publicly available.

(e) SUBMISSION TO CONGRESS.—

(1) DISCLOSURE POLICY AND REMEDIATION PROCESS.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to Congress a copy of the policy required under subsection (a) and the remediation process required under subsection (b).

(2) REPORT AND BRIEFING.—

(A) REPORT.—Not later than one year after establishing the policy required under subsection (a), the Secretary of Homeland Security shall submit to Congress a report on such policy and the remediation process required under subsection (b).

(B) ANNUAL BRIEFINGS.—One year after the date of the submission of the report under subparagraph (A), and annually thereafter for each of the next three years, the Secretary of Homeland Security shall provide to Congress a briefing on the policy required under subsection (a) and the process required under subsection (b).

(C) MATTERS FOR INCLUSION.—The report required under subparagraph (A) and the briefings required under subparagraph (B) shall include each of the following with respect to the policy required under subsection (a) and the process required under subsection (b) for the period covered by the report or briefing, as the case may be:

(i) The number of unique security vulnerabilities reported.

(ii) The number of previously unknown security vulnerabilities mitigated or remediated.

(iii) The number of unique individuals, organizations, and companies that reported security vulnerabilities.

(iv) The average length of time between the reporting of security vulnerabilities and mitigation or remediation of such vulnerabilities.

(f) DEFINITIONS.—In this section:

(1) The term "security vulnerability" has the meaning given that term in section 102(17) of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501(17)), in information technology.

(2) The term "information system" has the meaning given that term by section 3502(12) of title 44, United States Code.

(3) The term "appropriate information system" means an information system that the Secretary of Homeland Security selects for inclusion under the vulnerability disclosure policy required by subsection (a).

PURPOSE AND SUMMARY

H.R. 6735, the "Public-Private Cybersecurity Cooperation Act" requires the Secretary of Homeland Security to establish a policy for the reporting and remediation of security vulnerabilities on appropriate information systems within 90 days. The policy must include an understanding of the information technology that the policy applies to, the conditions under which individuals or organizations legally may discover and report vulnerabilities, and how those vulnerabilities are to be reported and disclosed.

Additionally, the bill requires the Department to identify a process that it must go through in mitigating and remediating security vulnerabilities. In developing the policy, the Secretary must consult with the Attorney General, the Secretary of Defense, the Administrator of the General Services Administration, and non-governmental security researchers. Finally, the bill lays out the specifics for reporting the policy to Congress, as well as a report to Congress on the effectiveness of the policy.

BACKGROUND AND NEED FOR LEGISLATION

In 2016, the Defense Digital Service (DDS) within the Department of Defense (DOD) created the "Hack the Pentagon Bug Bounty Program" which allowed civic-minded security researchers the opportunity to report vulnerabilities found on DOD websites. Following the "Hack the Pentagon program", DDS created a Vulnerability Disclosure Policy that allowed individuals and organizations the ability to submit vulnerabilities found on DOD websites through an online portal. The ability of the DOD to leverage the public in finding vulnerabilities in public websites enabled a greater understanding of DOD's public facing cybersecurity risks.

Based on the model and experience of DOD's vulnerability disclosure policy, this legislation would direct the Department to develop its own vulnerability disclosure policy. It is accepted industry practice among major technology companies to use vulnerability disclosure programs and bug bounty programs to help ensure the safety and security of their websites and platforms. Threat researchers from the private sector have commented on the process of receiving, reviewing, and responding to vulnerability disclosures as a foundational element of the modern cybersecurity policy.

Members of the Committee have expressed concerns over the Department's lack of a vulnerability disclosure policy, at both Full Committee hearings and in correspondence with the Department. To date, the Department has no legal avenue for people to report vulnerabilities found of the Department's websites. As the government faces ongoing threats to its online infrastructure, the goal of this legislation is to engage the public to be proactive with security concerns and improve its cybersecurity efforts.

H.R. 6735 directs the Secretary of Homeland Security to develop and implement a vulnerability disclosure program to keep pace with the constantly evolving threats the Department faces. Additionally, H.R. 6735 will ensure that the Department continues to

lead by example in the government's efforts to improve its cybersecurity posture.

HEARINGS

While the committee did not hold any hearings on H.R. 6735 directly, the following hearings touched on oversight authority:

March 9, 2017—Cybersecurity, Infrastructure Protection and Security Subcommittee: "The Current State of DHS Private Sector Engagement for Cybersecurity"

March 22, 2017—Full Committee: "A Borderless Battle: Defending Against Cyber Threats"

March, 28, 2017—Cybersecurity, Infrastructure Protection and Security Subcommittee: "The Current State of DHS' Efforts to Secure Federal Networks"

October 3, 2017—Cybersecurity, Infrastructure Protection and Security Subcommittee: "Examining DHS' Cybersecurity Mission"

November 15, 2017—Cybersecurity, Infrastructure Protection and Security Subcommittee: "Maximizing the Value of Cyber Threat Information Sharing"

April 26, 2018—Full Committee: "Strengthening the Safety and Security of Our Nation: The President's FY2019 Budget Request for the Department of Homeland Security"

July 25, 2018—Cybersecurity, Infrastructure Protection and Security Subcommittee: "Assessing the State of Federal Cybersecurity Risk Determination"

COMMITTEE CONSIDERATION

The Committee met on September 13, 2018, to consider H.R. 6735 and ordered the measure to be reported to the House with a favorable recommendation, amended, by unanimous consent. The Committee took the following actions:

The following amendments were offered:

An Amendment offered by Mr. RATCLIFFE and Mr. LANGEVIN (#1); was AGREED TO by unanimous consent.

Consisting of the following amendments:

This amendment amends the long title to read: "A bill to direct the Secretary of Homeland Security to establish a vulnerability disclosure policy for appropriate information systems of the Department of Homeland Security, and for other purposes."

Creates the short title: "Public-Private Cybersecurity Cooperation Act".

Page 2, lines 1 through 2, strike "Department of Homeland Security public internet websites that shall include" and insert "appropriate information systems of the Department of Homeland Security. Such policy shall include each of the following:".

Page 2, lines 3 through 4, strike "the information technology to which the policy applies" and insert "The appropriate information systems of the Department that individuals, organizations, and companies may use to discover and report security vulnerabilities on appropriate information systems".

In addition, makes technical corrections and updates the disclosure policy and remediation process.

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. 6735.

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. 6735 the "Public-Private Cybersecurity Cooperation Act", 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. 6735 contains the following general performance goals and objectives, including outcome related goals and objectives authorized.

H.R. 6735 requires the Secretary of Homeland Security to provide the vulnerability disclosure policy to Congress, and report to Congress on a variety of metrics related to the efficiency and success of vulnerability reporting and mitigation.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 6735 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. 6735 does not preempt any State, local, or Tribal law.

DISCLOSURE OF DIRECTED RULE MAKINGS

The Committee estimates that H.R. 6735 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 "Public-Private Cybersecurity Cooperation Act".

Sec. 2. Department of Homeland Security disclosure of security vulnerabilities

Section 1(a) requires the Secretary of Homeland Security (the Secretary) to establish a policy for individuals, organizations, and companies to report security vulnerabilities on Department of Homeland Security (DHS) appropriate information systems. The vulnerability disclosure policy required shall include: the applicable information technology; conditions and criteria under which individuals, organizations, and companies may legally operate and report security vulnerabilities; how vulnerabilities can be disclosed to DHS; how DHS will communicate with the parties that discover vulnerabilities; and how DHS or individuals can report security vulnerabilities. The Committee intends that the policy developed by the Department take into account the process for communicating vulnerabilities with the original manufacturer of the technology.

Section (b) requires the Secretary to develop a process for DHS to mitigate or remediate security vulnerabilities reported through the policy.

Section (c) requires the Secretary to consult with the Attorney General, Secretary of Defense and Administrator of the General Services Administration, as well as non-governmental security researchers when developing the vulnerability disclosure policy.

Section (d) requires the Secretary to make the vulnerability disclosure policy publicly available. The Committee intends lessons learned from other agencies that have existing security vulnerability disclosure programs be incorporated into DHS' policy. Additionally, the Committee intends that, to the extent security vulnerabilities reported to the Department are present in non-Department information systems, those vulnerabilities should be shared with participants in the Department's information sharing programs, including other federal agencies.

The Secretary is required under section (e) to submit the policy to Congress within 90 days, additionally the Secretary has to submit an annual report for three years (e)(2), on the number of unique security vulnerabilities reports, the number of previously unknown security vulnerabilities mitigated or remediated, the number of unique parties that reported security vulnerabilities, and the average length of time between the reporting of the security vulnerability and when it was mitigated or remediated.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

As reported, H.R. 6735 makes no changes to existing law.

○