115TH CONGRESS
2d Session

HOUSE OF REPRESENTATIVES

REPORT
115–964

HACK THE DEPARTMENT OF HOMELAND SECURITY ACT OF 2018

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

REPORT

[To accompany S. 1281]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the Act (S. 1281) to establish a bug bounty pilot program within the Department of Homeland Security, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the Act 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	6
Duplicative Federal Programs	6
Congressional Earmarks, Limited Tax Benefits, and Limited Tariff Benefits	6
Federal Mandates Statement	6
Preemption Clarification	6
Disclosure of Directed Rule Makings	7
Advisory Committee Statement	7
Applicability to Legislative Branch	7
Section-by-Section Analysis of the Legislation	7
Changes in Existing Law Made by the Bill, as Reported	8

The amendment is as follows:

Strike all after the enacting clause and insert the following:

79–006

SECTION 1. SHORT TITLE.

This Act may be cited as the "Hack the Department of Homeland Security Act of 2018" or the "Hack DHS Act".

SEC. 2. DEPARTMENT OF HOMELAND SECURITY BUG BOUNTY PILOT PROGRAM.

(a) DEFINITIONS.—In this section:

(1) BUG BOUNTY PROGRAM.—The term "bug bounty program" means a program under which—

(A) individuals, organizations, and companies are temporarily authorized to identify and report vulnerabilities of appropriate information systems of the Department; and

(B) eligible individuals, organizations, and companies receive compensation in exchange for such reports.

(2) DEPARTMENT.—The term "Department" means the Department of Homeland Security.

(3) ELIGIBLE INDIVIDUAL, ORGANIZATION, OR COMPANY.—The term "eligible individual, organization, or company" means an individual, organization, or company that meets such criteria as the Secretary determines in order to receive compensation in compliance with Federal laws.

(4) INFORMATION SYSTEM.—The term "information system" has the meaning given that term by section 3502 of title 44, United States Code.

(5) PILOT PROGRAM.—The term "pilot program" means the bug bounty pilot program required to be established under subsection (b)(1).

(6) SECRETARY.—The term "Secretary" means the Secretary of Homeland Security.

(b) ESTABLISHMENT OF PILOT PROGRAM.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Secretary shall establish, within the Office of the Chief Information Officer, a bug bounty pilot program to minimize vulnerabilities of appropriate information systems of the Department.

(2) REQUIREMENTS.—In establishing and conducting the pilot program, the Secretary shall—

(A) designate appropriate information systems to be included in the pilot program;

(B) provide compensation to eligible individuals, organizations, and companies for reports of previously unidentified security vulnerabilities within the information systems designated under subparagraph (A);

(C) establish criteria for individuals, organizations, and companies to be considered eligible for compensation under the pilot program in compliance with Federal laws;

(D) consult with the Attorney General on how to ensure that approved individuals, organizations, or companies that comply with the requirements of the pilot program are protected from prosecution under section 1030 of title 18, United States Code, and similar provisions of law, and civil lawsuits for specific activities authorized under the pilot program;

(E) consult with the Secretary of Defense and the heads of other departments and agencies that have implemented programs to provide compensation for reports of previously undisclosed vulnerabilities in information systems, regarding lessons that may be applied from such programs; and

(F) develop an expeditious process by which an individual, organization, or company can register with the Department, submit to a background check as determined by the Department, and receive a determination as to eligibility; and

(G) engage qualified interested persons, including non-government sector representatives, about the structure of the pilot program as constructive and to the extent practicable.

(3) CONTRACT.—In establishing the pilot program, the Secretary, subject to the availability of appropriations, may award one or more competitive contracts to an entity, as necessary, to manage the pilot program.

(c) REPORT.—Not later than 180 days after the date on which the pilot program is completed, 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 Representatives a report on the pilot program, which shall include—

(1) the number of individuals, organizations, or companies that participated in the pilot program, broken down by the number of individuals, organizations, or companies that—

(A) registered;

(B) were determined eligible;

(C) submitted security vulnerabilities; and

(D) received compensation;

(2) the number and severity of vulnerabilities reported as part of the pilot program;

(3) the number of previously unidentified security vulnerabilities remediated as a result of the pilot program;

(4) the current number of outstanding previously unidentified security vulnerabilities and Department remediation plans;

(5) the average length of time between the reporting of security vulnerabilities and remediation of the vulnerabilities;

(6) the types of compensation provided under the pilot program; and

(7) the lessons learned from the pilot program.

(d) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Department $250,000 for fiscal year 2019 to carry out this Act.

PURPOSE AND SUMMARY

S. 1281, the Hack the Department of Homeland Security Act of 2018, directs the Department of Homeland Security to establish a bug bounty pilot program within 180 days of enactment. To be located within the Office of the Chief Information Officer, the bug bounty program would allow participants to probe the appropriate information systems, as identified by the Department, to identify vulnerabilities. The pilot program authorizes the Secretary to provide compensation for reports of previously unidentified security vulnerabilities.

The bill addresses possible security concerns by directing the Secretary to designate appropriate information systems that should be included by the program. Additionally, the bill directs the Secretary to consult with the Attorney General to ensure program participants that comply with the requirements of the pilot program are protected from prosecution and to develop a background check process for eligible program participants. The bill requires the Department to submit a report, within 180 days upon completion of the program, to Congress providing an overview on the pilot program.

BACKGROUND AND NEED FOR LEGISLATION

A bug bounty program entails using white hat hackers to probe government systems looking for vulnerabilities and compensating any individual who may find one. The Department of Defense has been forward leaning on utilizing this tool, having run a pilot from April 18, 2016 to May 12, 2016 through its Defense Digital Services. Hosted by HackerOne, it included 1,410 participants who yielded 1,189 reports, the first of which came within 13 minutes. The entire cost of the 'Hack the Pentagon pilot' was $150,000, with about half going to the hackers themselves. Furthermore, the GSA launched a pilot program in August of 2017.

The White House has encouraged Federal Agencies to create bug bounty programs. The 2017 Report on Federal IT Modernization, identifies bug bounty programs as useful tools for providing visibility into Federal systems. In particular, bug bounty programs were highlighted "as a tool to expand visibility beyond the network level to provide security teams with other information feeds, which they can use to better understand, process, and triage information security events and possible incidents."

HEARINGS

While the committee didn't hold any hearings on 1281 directly, the following hearings addressed this issue:

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"

July 11, 2018—Full Committee: "DHS's Progress in Securing Election Systems and Other Critical Infrastructure"

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 S. 1281, and ordered the measure to be reported to the House with a favorable recommendation, amended, by unanimous consent.

The following amendments were offered:

An en bloc amendment offered by MR. LANGEVIN (#1E); was AGREED TO by unanimous consent.

Consisting of the following amendments:

This amendment defines: Bug Bounty Program as: (A) individuals, organizations, and companies are temporarily authorized to identify and report vulnerabilities of appropriate information systems of the Department; and (B) eligible individuals, organizations, and companies receive compensation in exchange for such reports.

Defines Eligible Individual organization or Company as: "an individual, organization, or company that meets such criteria as the Secretary determines in order to receive compensation in compliance with Federal laws."

Defines Information System as: "the meaning given that term by section 3502 of title 44, United States Code."

Page 3, beginning at line 5, strike "Internet-facing information technology" and insert "appropriate information systems".

Page 3, line 7, after "establishing" insert "and conducting".

Page 3, beginning at line 9, strike subparagraphs (A), (B), and (C) and insert the following:

(A) designate appropriate information systems to be included in the pilot program;

(B) provide compensation to eligible individuals, organizations, and companies for reports of previously unidentified security vulnerabilities within the information systems designated under subparagraph (A);

(C) establish criteria for individuals, organizations, and companies to be considered eligible for compensation under the pilot program in compliance with Federal laws;

Page 4, beginning at line 5, strike subparagraph (E) and insert a new subparagraph (E).

Page 4, after line 20, inserts information on the Secretary's ability to award contracts and makes technical changes.

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 S. 1281.

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 S. 1281, the Hack DHS 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, September 20, 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 S. 1281, the Hack DHS Act.

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

Sincerely,

KEITH HALL,
Director.

Enclosure.

S. 1281—Hack DHS Act

S. 1281 would direct the Department of Homeland Security to establish a pilot program to improve the security of the department's information technology systems. The act would authorize the appropriation of $250,000 for fiscal year 2019 for the pilot program. Assuming appropriation of that amount, CBO estimates that implementing S. 1281 would cost $250,000.

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

CBO estimates that enacting S. 1281 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2029.

S. 1281 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act.

On October 20, 2017, CBO transmitted a cost estimate for S. 1281 as ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on October 4, 2017. CBO's estimates of the budgetary effects of the two versions of the legislation are the same.

The CBO staff contact for this estimate is Mark Grabowicz. The estimate was reviewed 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, S. 1281 contains the following general performance goals and objectives, including outcome related goals and objectives authorized.

S. 1281 requires the Secretary of Homeland Security to establish a bug bounty pilot program within 180 days of enactment and to provide House and Senate Homeland Security Committees a report on the effectiveness of the pilot program.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that S. 1281 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 S. 1281 does not preempt any State, local, or Tribal law.

DISCLOSURE OF DIRECTED RULE MAKINGS

The Committee estimates that S. 1281 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 specifies that this Act may be cited as the "Hack the Department of Homeland Security Act of 2018," or the "Hack DHS Act."

Sec. 2. Department of Homeland Security Bug Bounty Pilot Program

Section 2(a) provides definitions for the following terms: "bug bounty program," "Department," "information technology," "pilot program," and "Secretary."

Section 2(b) instructs the Secretary of Homeland Security to establish a bug bounty pilot program at DHS within 180 days of the bill's enactment. In establishing the pilot program, the Secretary will: designate which information systems will be included in the program; provide compensation for eligible individuals, organizations and companies for reporting vulnerabilities within eligible information systems; establish criteria to be considered eligible for compensation; seek advice from the Attorney General regarding how to ensure approved participants are protected from prosecution and civil lawsuits for approved activities within the pilot program; confer with DOD officials on lessons learned from previously implemented programs to provide compensation for reporting unknown vulnerabilities in information systems; develop a vetting process for individuals, organizations, or companies; and engage public and private sector experts on the structure of the pilot program and lessons learned. The Department is authorized to award one or more contracts to manage the pilot program.

Section 2(c) requires the Secretary to submit a report to the Senate Homeland Security and Governmental Affairs Committee and the House of Representatives Committee on Homeland Security within 90 days of the completion of the pilot program. The report shall include a number of data points to assist Congress in assessing the pilot programs effectiveness, including, but not limited to: the number of pilot program participants that registered, were deemed eligible, submitted vulnerabilities, and received compensation; the quantity and severity of vulnerabilities identified; the number of unidentified vulnerabilities that were patched as a result of the pilot program; the number of vulnerabilities that have yet to be patched and the Department's plans to do so; how long it takes to report the vulnerability and to patch the vulnerability; the types of compensation provided for discovering undisclosed security vulnerabilities; and any lessons learned. The Committee intends for the Department to decide the value of vulnerabilities found, and offer monetary or other forms of compensation reasonably proportional to the value of the previously unidentified security vulnerability.

Section 2(d) authorizes $250,000 to be appropriated to DHS for fiscal year 2019 to carry out the pilot program.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

As reported S. 1281 makes no changes to existing law.

○