Calendar No. 335

115TH CONGRESS
2d Session

SENATE

REPORT
115–209

HACK THE DEPARTMENT OF HOMELAND SECURITY ACT

REPORT

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 1281

TO ESTABLISH A BUG BOUNTY PILOT PROGRAM WITHIN THE DEPARTMENT OF HOMELAND SECURITY, AND FOR OTHER PURPOSES

FEBRUARY 26, 2018.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
79–010 WASHINGTON : 2018

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

JOHN McCAIN, Arizona
ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MICHAEL B. ENZI, Wyoming
JOHN HOEVEN, North Dakota
STEVE DAINES, Montana

CLAIRE McCASKILL, Missouri
THOMAS R. CARPER, Delaware
HEIDI HEITKAMP, North Dakota
GARY C. PETERS, Michigan
MAGGIE HASSAN, New Hampshire
KAMALA D. HARRIS, California
DOUG JONES, Alabama

Christopher R. Hixon, *Staff Director*
Gabrielle D'Adamo Singer, *Chief Counsel*
Colleen E. Berny, *Research Assistant*
Maurice R. Turner, *Fellow*
Margaret E. Daum, *Minority Staff Director*
Stacia M. Cardille, *Minority Chief Counsel*
Charles A. Moskowitz, *Minority Senior Legislative Counsel*
Julie G. Klein, *Minority Professional Staff Member*
Laura W. Kilbride, *Chief Clerk*

Calendar No. 335

115TH CONGRESS 2d Session | SENATE | REPORT 115–209

HACK THE DEPARTMENT OF HOMELAND SECURITY ACT

FEBRUARY 26, 2018.—Ordered to be printed

Mr. JOHNSON, from the Committee on Homeland Security and Governmental Affairs, submitted the following

REPORT

[To accompany S. 1281]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 1281), to establish a bug bounty pilot program within the Department of Homeland Security, and for other purposes, reports favorably thereon with an amendment and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

S. 1281, the Hack the Department of Homeland Security Act of 2017, or the Hack DHS Act, directs the Secretary of Homeland Security (Secretary) to establish a bug bounty pilot program at the Department of Homeland Security (DHS or the Department) to enhance the Department's cybersecurity by minimizing vulnerabilities to public-facing information technology.

The bill also requires the Secretary to ensure compensation is awarded to participants for identifying undisclosed vulnerabilities during the pilot program, and to award contracts to manage the pilot program and patch vulnerabilities, among other things. Lastly, the bill requires the Secretary to submit a report to Congress on the pilot program and its findings.

II. BACKGROUND AND THE NEED FOR LEGISLATION

In early 2017, then-Secretary John Kelly stated that "[c]yber threats present a tremendous danger to our American way of life. The consequences of these digital threats are no less significant than threats in the physical world."[1] One report found that, in 2016, just one anti-virus software company blocked over 229,000 web attacks every day.[2] In addition, "[m]ore than three-quarters (76 percent) of scanned websites in 2016 contained vulnerabilities, nine percent of which were deemed critical."[3] Bug bounty programs can identify these types of vulnerabilities before they are exploited, and have proven beneficial in both the public and private sectors.

Private sector bug bounty programs

Although bug bounty programs vary in composition, incentives, and purpose, generally speaking a bug bounty program provides incentives to participants to identify vulnerabilities in an information technology program or system. Individuals, organizations, or companies are incentivized through various forms of payouts or nonmonetary compensation to detect new and valid vulnerabilities on information technology and systems. Some examples of rewards include recognition, cash, and gifts.[4] Bug bounty programs have been used by the private sector for over 20 years; however, their use has rapidly increased in recent years.[5] According to one company's report tracking bug bounty programs, there have been "three times more enterprise bug bounty programs launched in the past year than the previous three years combined."[6] In addition, since 2016, the average monetary payout has increased by 53 percent, averaging $451.[7] Between 2016 and 2017, hundreds of private and public bug bounty programs have identified over 52,000 valid vulnerabilities, a high watermark, and critical vulnerabilities identification increased by 25 percent.[8]

Bug bounties have helped the private sector increase security. For example, Microsoft has utilized bug bounty programs since 2013.[9] According to Microsoft, "[t]hese bounty programs help Microsoft harness the collective intelligence and capabilities of security researchers to help protect customers."[10] In 2016, Microsoft

[1] Press Release, Dep't of Homeland Sec., Home and Away: DHS and the Threats to America (Apr. 18, 2017), https://www.dhs.gov/news/2017/04/18/home-and-away-dhs-and-threats-america. Remarks delivered by Secretary Kelly at George Washington University Center for Cyber and Homeland Security.

[2] Symantec Corp., *Internet Security Threat Report,* 7 (2017), https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf.

[3] *Id.*

[4] *Id.*

[5] Bugcrowd, *The Adoption of Bug Bounties in the Financial Services Industry,* Bugcrowd Industry Report 1 (2016), https://pages.bugcrowd.com/hubfs/PDFs/Financial-Services-Spotlight.pdf?t=1507846659848.

[6] Bugcrowd, *2017 State of Bug Bounty Report* (2017), https://pages.bugcrowd.com/hubfs/Bugcrowd-2017-State-of-Bug-Bounty-Report.pdf (quoting an excerpt from the Executive Summary).

[7] *Id.*

[8] *Id.*

[9] *Microsoft Bounty Programs,* Microsoft Security TechCenter, https://technet.microsoft.com/en-us/security/dn425036 (last visited Nov. 7, 2017).

[10] *Id.*

launched a bug bounty program for Windows, with monetary awards ranging from $500 to $250,000.[11] Microsoft currently has nine active bug bounty programs.[12]

Public sector bug bounty programs

On March 2, 2016, the Department of Defense (DOD) announced the "Hack the Pentagon" initiative, the Federal Government's first bug bounty pilot program.[13] The bug bounty program was modeled after private sector programs and intended "to improve the security and delivery of networks, products, and digital services."[14] The pilot program ran from April 18, 2016, until May 12, 2016, and cost $150,000.[15] During the pilot program, out of more than 1,400 invited participants, 250 submitted vulnerability reports and 138 were deemed "legitimate, unique and eligible for a bounty."[16] On October 20, 2016, the DOD announced a "Hack the Pentagon" follow-up initiative.[17]

After the DOD's Hack the Pentagon's success, on November 11, 2016, the Secretary of the Army announced its own "Hack the Army" bug bounty program, which targeted the Army's operationally-significant websites.[18] The bug bounty program ran from November 30, 2016, to December 21, 2016.[19] Overall, participants submitted 416 reports, with 118 being deemed "unique and actionable."[20] The estimated total amount paid to the hackers that identified vulnerabilities was approximately $100,000.[21]

On April 26, 2017, the Air Force announced the "Hack the Air Force" bug bounty program.[22] The program ran from May 30, 2017, until June 23, 2017, with more than 270 participants.[23] Overall, 207 "valid vulnerabilities" were identified, and participants that identified vulnerabilities were collectively awarded more than $130,000.[24]

On May 9, 2017, the General Services Administration (GSA) established the first public bug bounty program run at a non-military

[11] Emil Protalinski, *Microsoft Launches Windows Bug Bounty Program with Rewards Ranging from $500 to $250,000,* Venture Beat (July 26, 2017), https://venturebeat.com/2017/07/26/microsoft-launches-windows-bug-bounty-program-with-rewards-ranging-from-500-to-250000.

[12] *Microsoft Bounty Programs, supra note 9.*

[13] Press Release, Dep't of Defense, Statement by Pentagon Press Secretary Peter Cook on DoD's "Hack the Pentagon" Cybersecurity Initiative (Mar. 2, 2016), https://www.defense.gov/News/News-Releases/News-Release-View/Article/684106/statement-by-pentagon-press-secretary-peter-cook-on-dods-hack-the-pentagon-cybe.

[14] *Id.*

[15] Lisa Ferdinando, *Carter Announces 'Hack the Pentagon' Program Results,* Dep't of Defense (June 17, 2016), https://www.defense.gov/News/Article/Article/802828/carter-announces-hack-the-pentagon-program-results.

[16] *Id.*

[17] Shannon Collins, *DOD Announces 'Hack the Pentagon' Follow-Up Initiative,* Dep't of Defense (Oct. 20, 2016), https://www.defense.gov/News/Article/Article/981160/dod-announces-hack-the-pentagon-follow-up-initiative.

[18] Maj. Christopher Ophardt, *Army Secretary Issues Challenge with 'Hack the Army' Program,* U.S. Army (Nov. 21, 2016), https://www.army.mil/article/178473/army_secretary_issues_challenge_with_hack_the_army_program.

[19] *Hack the Army Results Are In,* HackerOne (Jan. 19, 2017), https://www.hackerone.com/blog/Hack-The-Army-Results-Are-In.

[20] *Id.*

[21] *Id.*

[22] Press Release, Dep't of Defense, Air Force Issues Challenge to "Hack the Air Force" (Apr. 26, 2017), https://www.defense.gov/News/News-Releases/News-Release-View/Article/1164012/air-force-issues-challenge-to-hack-the-air-force.

[23] Rusty Frank, *Hack the Air Force Results Released,* U.S. Air Force (Aug. 10, 2017), http://www.af.mil/News/Article-Display/Article/1274518/hack-the-air-force-results-released.

[24] *Id.*

agency.[25] This bug bounty was developed in the same vein as the DOD programs, but runs on an on-going basis.[26] Since its announcement, GSA has identified and resolved 41 vulnerabilities, and paid out $12,600 in bounties ranging from $150 to $2,000.[27]

Entities are now working to institutionalize the public's ability to report discovered vulnerabilities. Following the start of the "Hack the Army" bug bounty program, DOD formalized how to report vulnerabilities discovered on their public-facing sites with the creation of the Vulnerability Disclosure Policy (VDP).[28] The VDP is "intended to give security researchers clear guidelines for conducting vulnerability discovery activities directed at [DOD] web properties, and submitting discovered vulnerabilities to DOD."[29] Former Defense Secretary Ash Carter described the VDP as "a 'see something, say something' policy for the digital domain."[30] The Department of Justice Computer Crime & Intellectual Property Section published its "Framework for a Vulnerability Disclosure Program for Online Systems" on August 1, 2017.[31] The framework is designed to help businesses and other organizations develop a formal vulnerability disclosure program that allows researchers to legally participate without running afoul of the Computer Fraud and Abuse Act.[32]

Need at the Department of Homeland Security

DHS is "responsible for protecting civilian federal government networks and collaborating with other Federal agencies, as well as State, local, tribal, and territorial governments, and the private sector to defend against cyber threats."[33] In addition to cybersecurity, the Department is responsible for a variety of missions, including preventing terrorism, border security, and disaster resilience. As a result, it is essential that the Department's information technology is secure and resilient.

The Federal Government, including DHS, faces daily cyber threats from a variety of adversaries. In 2016, there were over 30,899 cyber incidents at Federal agencies.[34] DHS reported 1,112

[25] Omid Ghaffari-Tabrizi, Waldo Jaquith and Eric Mill, *The next step towards a bug bounty program for the Technology Transformation Service,* 18F Digital Service Agency, Government Service Administration, (May 11, 2017), https://18f.gsa.gov/2017/05/11/the-next-steps-towards-bug-bounty-program-for-technology-transformation-service/.

[26] *Id.*

[27] *TTS Bug Bounty: The First Civilian Agency Public Bug Bounty Program,* HackerOne, https://hackerone.com/tts (last visited Jan. 23, 2018).

[28] *Hack the Pentagon,* HackerOne, https://www.hackerone.com/resources/hack-the-pentagon (last visited Oct. 20, 2017).

[29] *U.S. Dep't of Defense,* HackerOne, https://hackerone.com/deptofdefense (last visited Oct. 20, 2017).

[30] *Hack the Pentagon, supra* note 28.

[31] Press Release, U.S. Computer Emergency Readiness Team, DOJ Provides Organizations a Framework for Development of a Vulnerability Disclosure Program (Aug. 1, 2017), https://www.us-cert.gov/ncas/current-activity/2017/08/01/DOJ-Provides-Organizations-Framework-Development-Vulnerability; *see also* Cybersecurity Unit, *A Framework for a Vulnerability Disclosure Program for Online Systems,* U.S. Dep't of Justice, https://www.justice.gov/criminal-ccips/page/file/983996/download.

[32] Cybersecurity Unit, *supra* note 31 at 1–2.

[33] *Examining DHS's Cybersecurity Mission Before the Cybersecurity and Infrastructure Protection Subcomm. of the H. Homeland Security Comm.,* 115th Cong. 1 (2017) (statement of Assistant Sec'y for Cybersecurity & Comm'ns Nat'l Prot. & Programs Directorate U.S. Dep't of Homeland Sec.), *available at* http://docs.house.gov/meetings/HM/HM08/20171003/106448/HHRG-115-HM08-Wstate-ManfraJ-20171003.pdf.

[34] Executive Office of the President of the United States, Federal Information Security Modernization Act of 2014, Annual Report to Congress, Fiscal Year 2016, https://www.whitehouse.gov/sites/whitehouse.gov/files/briefing-room/presidential-actions/related-omb-material/fy_2016_fisma_report%20to_congress_official_release_march_10_2017.pdf (last visited Dec. 1, 2017).

incidents, which is comparable to the 1,888 reported by DOD.[35] The DHS Inspector General additionally found that Department "components were not consistently following DHS's policies and procedures to maintain current or complete information on remediating security weaknesses in a timely manner." [36]

In recognition of this serious threat, the Committee has made cybersecurity one of its top priorities. From 2015 through 2017, the Committee held five hearings on cybersecurity, exploring topics such as information sharing, data breaches in the Federal Government, and how adversaries continue to target information networks.[37] The Committee has also passed multiple pieces of cybersecurity legislation, including the Federal Cybersecurity Enhancement Act of 2015, to improve Federal network security and authorize and enhance the EINSTEIN intrusion detection and prevention system.[38]

The relative success of the bug bounty programs in the private sector, DOD and GSA, as well as findings by the DHS Inspector General, suggest the need for DHS to pursue a similar pilot program to identify vulnerabilities on Internet-facing information technology. This legislation requires DHS to establish a one-time bug bounty pilot program under which approved individuals, organizations, or companies can detect and patch vulnerabilities and receive compensation. Based on the findings, the Department can then determine if a permanent program is needed.

III. LEGISLATIVE HISTORY

Senator Margaret Wood Hassan (D–NH) introduced S. 1281, the Hack the Department of Homeland Security Act of 2017, on May 25, 2017. Senators Claire McCaskill (D–MO), Rob Portman (R–OH), and Kamala Harris (D–CA) are cosponsors.

The bill was referred to the Committee on Homeland Security and Governmental Affairs. The Committee considered S. 1281 at a business meeting on October 4, 2017. Senator Hassan offered a substitute amendment that made minor revisions to the bill, including clarifying the definition and requirements of the bug bounty program. The substitute amendment was adopted by unanimous consent with Senators Johnson, Lankford, Daines, McCaskill, Tester, Heitkamp, Hassan, and Harris present.

The Committee favorably reported the bill as amended by the Hassan substitute amendment by voice vote *en bloc*. Senators present for the vote were Johnson, Lankford, Daines, McCaskill, Tester, Heitkamp, Hassan, and Harris.

[35] *Id.*

[36] *Id.* at 45.

[37] *Cybersecurity Regulation Harmonization: Hearing before the S. Comm. On Homeland Sec. & Governmental Affairs,* 115th Cong. (2017); *Cyber Threats Facing America: An Overview of the Cybersecurity Threat Landscape: Hearing before the S. Comm. On Homeland Sec. & Governmental Affairs*, 115th Cong. (2017); *Under Attack: Federal Cybersecurity and the OPM Data Breach: Hearing before the S. Comm. On Homeland Sec. & Governmental Affairs,* 114th Cong. (2015); *The IRS Data Breach: Steps to Protect Americans' Personal Information: Hearing before the S. Comm. On Homeland Sec. & Governmental Affairs,* 114th Cong. (2015); *Protecting America from Cyberattacks: The Importance of Information Sharing: Hearing before the S. Comm. On Homeland Sec. & Governmental Affairs,* 114th Cong. (2015).

[38] Public Law No: 114–113 (S. 1869, with amendments, was included in H.R. 2029).

IV. SECTION-BY-SECTION ANALYSIS OF THE BILL, AS REPORTED

Section 1. Short title

This section provides the bill's title, the "Hack the Department of Homeland Security Act of 2017," 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: ensure compensation is awarded to participants for identifying undisclosed vulnerabilities during the pilot program; award a contract to manage the pilot program and patch identified vulnerabilities; decide which mission-critical information technology should not be included in the pilot program; seek advice from the Attorney General regarding how to ensure approved participants are protected from prosecution for their approved activities within the pilot program; confer with DOD officials on lessons learned from launching "Hack the Pentagon" in 2016; develop a vetting process for approved participants; and engage public and private sector experts on the structure of the pilot program and lessons learned.

Section 2(c) requires the Secretary to submit a report to the U.S. Senate Homeland Security and Governmental Affairs Committee and the U.S. House Committee on Homeland Security within 90 days of the pilot program's completion. 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 approved, 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.

Section 2(d) authorizes $250,000 to be appropriated to DHS for fiscal year 2018 to carry out the pilot program.

V. EVALUATION OF REGULATORY IMPACT

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

VI. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, October 20, 2017.

Hon. RON JOHNSON,
Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate, 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 (DHS) to establish a pilot program to improve the security of the department's information technology systems, especially those that are accessible to the public (such as websites for the agencies within DHS). The bill would authorize the appropriation of $250,000 for fiscal year 2018 for the pilot program. Assuming appropriation of that amount, CBO estimates that implementing the bill would cost $250,000.

Enacting the bill 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 2028.

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

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

VII. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

Because this legislation would not repeal or amend any provision of current law, it would not make changes in existing law within the meaning of clauses (a) and (b) of paragraph 12 of rule XXVI of the Standing Rules of the Senate.

○