....
(Original Signature of Member)

115TH CONGRESS
2D SESSION

H. R. ____

To require the Secretary of State to design and establish a Vulnerability Disclosure Program (VDP) to improve Department of State cybersecurity and a bug bounty program to identify and report vulnerabilities of internet-facing information technology of the Department of State, and for other purposes.

———————————————

IN THE HOUSE OF REPRESENTATIVES

Mr. TED LIEU of California introduced the following bill; which was referred to the Committee on _____

———————————————

A BILL

To require the Secretary of State to design and establish a Vulnerability Disclosure Program (VDP) to improve Department of State cybersecurity and a bug bounty program to identify and report vulnerabilities of internet-facing information technology of the Department of State, and for other purposes.

1   *Be it enacted by the Senate and House of Representa-*

2 *tives of the United States of America in Congress assembled,*

SECTION 1. SHORT TITLE.

This Act may be cited as the "Hack Your State De-partment Act".

SEC. 2. DEFINITIONS.

In this Act:

(1) DEPARTMENT.—The term "Department" means the Department of Sate.

(2) INFORMATION TECHNOLOGY.—The term "information technology" has the meaning given such term in section 11101 of title 40, United States Code.

(3) SECRETARY.—The term "Secretary" means the Secretary of State.

SEC. 3. DEPARTMENT OF STATE VULNERABILITY DISCLO-SURE PROGRAM.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary shall de-sign, establish, and make publicly known a Vulnerability Disclosure Program (VDP) to improve Department cyber-security by—

(1) providing security researchers with clear guidelines for—

(A) conducting vulnerability discovery ac-tivities directed at Department information technology; and

1   (B)   submitting   discovered   security

2   vulnerabilities to the Department; and

3   (2) creating Department procedures and infra-

4   structure   to   receive   and   fix   discovered

5   vulnerabilities.

6   (b) REQUIREMENTS.—In establishing the VDP pur-

7 suant to paragraph (1), the Secretary shall—

8   (1)   identify   which   Department   information

9   technology should be included in the program;

10   (2)   determine   whether   the   program   should   dif-

11   ferentiate among and specify the types of security

12   vulnerabilities that may be targeted;

13   (3) provide a readily available means of report-

14   ing discovered security vulnerabilities and the form

15   in which such vulnerabilities should be reported;

16   (4) identify which Department offices and posi-

17   tions will be responsible for receiving, prioritizing,

18   and addressing security vulnerability disclosure re-

19   ports;

20   (5) consult with the Attorney General regarding

21   how to ensure that approved individuals, organiza-

22   tions, and companies that comply with the require-

23   ments of the program are protected from prosecu-

24   tion under section 1030 of title 18, United States

1 Code, and similar provisions of law for specific ac-

2 tivities authorized under the program;

3 (6) consult with the relevant offices at the De-

4 partment of Defense that were responsible for

5 launching the 2016 Vulnerability Disclosure Pro-

6 gram, "Hack the Pentagon", and subsequent De-

7 partment of Defense bug bounty programs;

8 (7) engage qualified interested persons, includ-

9 ing non-governmental sector representatives, about

10 the structure of the program as constructive and to

11 the extent practicable; and

12 (8) award a contract to an entity, as necessary,

13 to manage the program and implement the remedi-

14 ation of discovered security vulnerabilities.

15 (c) ANNUAL REPORTS.—Not later than 180 days

16 after the establishment of the VDP under subsection (a)

17 and annually thereafter for the next six years, the Sec-

18 retary of State shall submit to the Committee on Foreign

19 Affairs of the House of Representatives and the Com-

20 mittee on Foreign Relations of the Senate a report on the

21 following with respect to the VDP:

22 (1) The number and severity, in accordance

23 with the National Vulnerabilities Database of the

24 National Institute of Standards and Technology, of

25 security vulnerabilities reported.

5

1   (2) The number of previously unidentified secu-

2   rity vulnerabilities remediated as a result.

3   (3) The current number of outstanding pre-

4   viously unidentified security vulnerabilities and De-

5   partment of State remediation plans.

6   (4) The average length of time between the re-

7   porting of security vulnerabilities and remediation of

8   such vulnerabilities.

9   (5) An estimate of the total cost savings of dis-

10   covering and addressing security vulnerabilities sub-

11   mitted through the VDP.

12   (6) The resources, surge staffing, roles, and re-

13   sponsibilities within the Department used to imple-

14   ment the VDP and complete security vulnerability

15   remediation.

16   (7) Any other information the Secretary deter-

17   mines relevant.

18 **SEC. 4. DEPARTMENT OF STATE BUG BOUNTY PILOT PRO-**

19   **GRAM.**

20   (a) ESTABLISHMENT OF PILOT PROGRAM.—

21   (1) IN GENERAL.—Not later than one year

22   after the date of the enactment of this Act, the Sec-

23   retary shall establish a bug bounty pilot program to

24   minimize security vulnerabilities of internet-facing

25   information technology of the Department.

6

1   (2) REQUIREMENTS.—In establishing the pilot

2 program described in paragraph (1), the Secretary

3 shall—

4   (A) provide compensation for reports of

5 previously unidentified security vulnerabilities

6 within the websites, applications, and other

7 Internet-facing information technology of the

8 Department that are accessible to the public;

9   (B) award a contract to an entity, as nec-

10 essary, to manage such pilot program and for

11 executing the remediation of security

12 vulnerabilities identified pursuant to subpara-

13 graph (A);

14   (C) identify which Department information

15 technology should be included in such pilot pro-

16 gram;

17   (D) consult with the Attorney General on

18 how to ensure that approved individuals, orga-

19 nizations, or companies that comply with the

20 requirements of such pilot program are pro-

21 tected from prosecution under section 1030 of

22 title 18, United States Code, and similar provi-

23 sions of law for specific activities authorized

24 under such pilot program;

1 (E) consult with the relevant offices at the
2 Department of Defense that were responsible
3 for launching the 2016 "Hack the Pentagon"
4 pilot program and subsequent Department of
5 Defense bug bounty programs;

6 (F) develop a process by which an ap-
7 proved individual, organization, or company can
8 register with the entity referred to in subpara-
9 graph (B), submit to a background check as de-
10 termined by the Department, and receive a de-
11 termination as to eligibility for participation in
12 such pilot program; and

13 (G) engage qualified interested persons, in-
14 cluding non-governmental sector representa-
15 tives, about the structure of such pilot program
16 as constructive and to the extent practicable.

17 (b) REPORT.—Not later than 90 days after the date
18 on which the bug bounty pilot program under subsection
19 (a) is completed, the Secretary shall submit to the Com-
20 mittee on Foreign Relations of the Senate and the Com-
21 mittee on Foreign Affairs of the House of Representatives
22 a report on such pilot program, including information re-
23 lating to—

24 (1) the number of approved individuals, organi-
25 zations, or companies involved in such pilot pro-

8

1 gram, broken down by the number of approved indi-

2 viduals, organizations, or companies that—

3   (A) registered;

4   (B) were approved;

5   (C) submitted security vulnerabilities; and

6   (D) received compensation;

7   (2) the number and severity, in accordance with

8 the National Vulnerabilities Database of the Na-

9 tional Institute of Standards and Technology, of se-

10 curity vulnerabilities reported as part of such pilot

11 program;

12   (3) the number of previously unidentified secu-

13 rity vulnerabilities remediated as a result of such

14 pilot program;

15   (4) the current number of outstanding pre-

16 viously unidentified security vulnerabilities and De-

17 partment remediation plans;

18   (5) the average length of time between the re-

19 porting of security vulnerabilities and remediation of

20 such vulnerabilities;

21   (6) the types of compensation provided under

22 such pilot program; and

23   (7) the lessons learned from such pilot pro-

24 gram.