

116TH CONGRESS
1ST SESSION

H. R. 328

To require the Secretary of State to design and establish a Vulnerability Disclosure Process (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

JANUARY 8, 2019

Mr. TED LIEU of California (for himself and Mr. YOHO) introduced the following bill; which was referred to the Committee on Foreign Affairs

A BILL

To require the Secretary of State to design and establish a Vulnerability Disclosure Process (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,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Hack Your State De-
5 partment Act”.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) **BUG BOUNTY PROGRAM.**—The term “bug
4 bounty program” means a program under which an
5 approved individual, organization, or company is
6 temporarily authorized to identify and report
7 vulnerabilities of internet-facing information tech-
8 nology of the Department in exchange for compensa-
9 tion.

10 (2) **DEPARTMENT.**—The term “Department”
11 means the Department of State.

12 (3) **INFORMATION TECHNOLOGY.**—The term
13 “information technology” has the meaning given
14 such term in section 11101 of title 40, United
15 States Code.

16 (4) **SECRETARY.**—The term “Secretary” means
17 the Secretary of State.

18 **SEC. 3. DEPARTMENT OF STATE VULNERABILITY DISCLO-**
19 **SURE PROCESS.**

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

25 (1) providing security researchers with clear
26 guidelines for—

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

4 (B) submitting discovered security vulnera-
5 bilities to the Department; and

6 (2) creating Department procedures and infra-
7 structure to receive and fix discovered vulnerabili-
8 ties.

9 (b) REQUIREMENTS.—In establishing the VDP pur-
10 suant to paragraph (1), the Secretary shall—

11 (1) identify which Department information
12 technology should be included in the process;

13 (2) determine whether the process should dif-
14 ferentiate among and specify the types of security
15 vulnerabilities that may be targeted;

16 (3) provide a readily available means of report-
17 ing discovered security vulnerabilities and the form
18 in which such vulnerabilities should be reported;

19 (4) identify which Department offices and posi-
20 tions will be responsible for receiving, prioritizing,
21 and addressing security vulnerability disclosure re-
22 ports;

23 (5) consult with the Attorney General regarding
24 how to ensure that individuals, organizations, and
25 companies that comply with the requirements of the

1 process are protected from prosecution under section
2 1030 of title 18, United States Code, and similar
3 provisions of law for specific activities authorized
4 under the process;

5 (6) consult with the relevant offices at the De-
6 partment of Defense that were responsible for
7 launching the 2016 Vulnerability Disclosure Pro-
8 gram, “Hack the Pentagon”, and subsequent De-
9 partment of Defense bug bounty programs;

10 (7) engage qualified interested persons, includ-
11 ing nongovernmental sector representatives, about
12 the structure of the process as constructive and to
13 the extent practicable; and

14 (8) award contracts to entities, as necessary, to
15 manage the process and implement the remediation
16 of discovered security vulnerabilities.

17 (c) ANNUAL REPORTS.—Not later than 180 days
18 after the establishment of the VDP under subsection (a)
19 and annually thereafter for the next six years, the Sec-
20 retary of State shall submit to the Committee on Foreign
21 Affairs of the House of Representatives and the Com-
22 mittee on Foreign Relations of the Senate a report on the
23 VDP, including information relating to the following:

24 (1) The number and severity, in accordance
25 with the National Vulnerabilities Database of the

1 National Institute of Standards and Technology, of
2 security vulnerabilities reported.

3 (2) The number of previously unidentified secu-
4 rity vulnerabilities remediated as a result.

5 (3) The current number of outstanding pre-
6 viously unidentified security vulnerabilities and De-
7 partment of State remediation plans.

8 (4) The average length of time between the re-
9 porting of security vulnerabilities and remediation of
10 such vulnerabilities.

11 (5) The resources, surge staffing, roles, and re-
12 sponsibilities within the Department used to imple-
13 ment the VDP and complete security vulnerability
14 remediation.

15 (6) Any other information the Secretary deter-
16 mines relevant.

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

19 (a) ESTABLISHMENT OF PILOT PROGRAM.—

20 (1) IN GENERAL.—Not later than one year
21 after the date of the enactment of this Act, the Sec-
22 retary shall establish a bug bounty pilot program to
23 minimize security vulnerabilities of internet-facing
24 information technology of the Department.

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 contracts to entities, as nec-
10 essary, to manage such pilot program and for
11 executing the remediation of security vulnerabil-
12 ities identified pursuant to subparagraph (A);

13 (C) identify which Department information
14 technology should be included in such pilot pro-
15 gram;

16 (D) consult with the Attorney General on
17 how to ensure that individuals, organizations,
18 or companies that comply with the requirements
19 of such pilot program are protected from pros-
20 ecution under section 1030 of title 18, United
21 States Code, and similar provisions of law for
22 specific activities authorized under such pilot
23 program;

24 (E) consult with the relevant offices at the
25 Department of Defense that were responsible

1 for launching the 2016 “Hack the Pentagon”
2 pilot program and subsequent Department of
3 Defense bug bounty programs;

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

11 (G) engage qualified interested persons, in-
12 cluding nongovernmental sector representatives,
13 about the structure of such pilot program as
14 constructive and to the extent practicable; and

15 (H) consult with relevant United States
16 Government officials to ensure that such pilot
17 program complements persistent network and
18 vulnerability scans of the Department of State’s
19 internet-accessible systems, such as the scans
20 conducted pursuant to Binding Operational Di-
21 rective BOD–15–01.

22 (3) DURATION.—The pilot program established
23 under paragraph (1) should be short-term in dura-
24 tion and not last longer than one year.

1 (b) REPORT.—Not later than 180 days after the date
2 on which the bug bounty pilot program under subsection
3 (a) is completed, the Secretary shall submit to the Com-
4 mittee on Foreign Relations of the Senate and the Com-
5 mittee on Foreign Affairs of the House of Representatives
6 a report on such pilot program, including information re-
7 lating to—

8 (1) the number of approved individuals, organi-
9 zations, or companies involved in such pilot pro-
10 gram, broken down by the number of approved indi-
11 viduals, organizations, or companies that—

12 (A) registered;

13 (B) were approved;

14 (C) submitted security vulnerabilities; and

15 (D) received compensation;

16 (2) the number and severity, in accordance with
17 the National Vulnerabilities Database of the Na-
18 tional Institute of Standards and Technology, of se-
19 curity vulnerabilities reported as part of such pilot
20 program;

21 (3) the number of previously unidentified secu-
22 rity vulnerabilities remediated as a result of such
23 pilot program;

1 (4) the current number of outstanding pre-
2 viously unidentified security vulnerabilities and De-
3 partment remediation plans;

4 (5) the average length of time between the re-
5 porting of security vulnerabilities and remediation of
6 such vulnerabilities;

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

9 (7) the lessons learned from such pilot pro-
10 gram.

○