116TH CONGRESS
1ST SESSION

H. R. 328

AN ACT

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".

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

8 (1) BUG BOUNTY PROGRAM.—The term "bug
9 bounty program" means a program under which an
10 approved individual, organization, or company is
11 temporarily authorized to identify and report
12 vulnerabilities of internet-facing information tech-
13 nology of the Department in exchange for compensa-
14 tion.

15 (2) DEPARTMENT.—The term "Department"
16 means the Department of State.

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

21 (4) SECRETARY.—The term "Secretary" means
22 the Secretary of State.

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

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary shall design, establish, and make publicly known a Vulnerability Disclosure Process (VDP) to improve Department cybersecurity by—

(1) providing security researchers with clear guidelines for—

(A) conducting vulnerability discovery activities directed at Department information technology; and

(B) submitting discovered security vulnerabilities to the Department; and

(2) creating Department procedures and infrastructure to receive and fix discovered vulnerabilities.

(b) REQUIREMENTS.—In establishing the VDP pursuant to paragraph (1), the Secretary shall—

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

(2) determine whether the process should differentiate among and specify the types of security vulnerabilities that may be targeted;

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

2 ing discovered security vulnerabilities and the form

3 in which such vulnerabilities should be reported;

4   (4) identify which Department offices and posi-

5 tions will be responsible for receiving, prioritizing,

6 and addressing security vulnerability disclosure re-

7 ports;

8   (5) consult with the Attorney General regarding

9 how to ensure that individuals, organizations, and

10 companies that comply with the requirements of the

11 process are protected from prosecution under section

12 1030 of title 18, United States Code, and similar

13 provisions of law for specific activities authorized

14 under the process;

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

16 partment of Defense that were responsible for

17 launching the 2016 Vulnerability Disclosure Pro-

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

19 partment of Defense bug bounty programs;

20   (7) engage qualified interested persons, includ-

21 ing nongovernmental sector representatives, about

22 the structure of the process as constructive and to

23 the extent practicable; and

1   (8) award contracts to entities, as necessary, to

2   manage the process and implement the remediation

3   of discovered security vulnerabilities.

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

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

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

7 retary of State shall submit to the Committee on Foreign

8 Affairs of the House of Representatives and the Com-

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

10 VDP, including information relating to the following:

11   (1) The number and severity, in accordance

12   with the National Vulnerabilities Database of the

13   National Institute of Standards and Technology, of

14   security vulnerabilities reported.

15   (2) The number of previously unidentified secu-

16   rity vulnerabilities remediated as a result.

17   (3) The current number of outstanding pre-

18   viously unidentified security vulnerabilities and De-

19   partment of State remediation plans.

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

21   porting of security vulnerabilities and remediation of

22   such vulnerabilities.

23   (5) The resources, surge staffing, roles, and re-

24   sponsibilities within the Department used to imple-

1 ment the VDP and complete security vulnerability

2 remediation.

3   (6) Any other information the Secretary deter-

4 mines relevant.

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

6   **GRAM.**

7 (a) ESTABLISHMENT OF PILOT PROGRAM.—

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

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

10 retary shall establish a bug bounty pilot program to

11 minimize security vulnerabilities of internet-facing

12 information technology of the Department.

13   (2) REQUIREMENTS.—In establishing the pilot

14 program described in paragraph (1), the Secretary

15 shall—

16   (A) provide compensation for reports of

17   previously unidentified security vulnerabilities

18   within the websites, applications, and other

19   internet-facing information technology of the

20   Department that are accessible to the public;

21   (B) award contracts to entities, as nec-

22   essary, to manage such pilot program and for

23   executing the remediation of security vulnerabil-

24   ities identified pursuant to subparagraph (A);

1   (C) identify which Department information

2   technology should be included in such pilot pro-

3   gram;

4   (D) consult with the Attorney General on

5   how to ensure that individuals, organizations,

6   or companies that comply with the requirements

7   of such pilot program are protected from pros-

8   ecution under section 1030 of title 18, United

9   States Code, and similar provisions of law for

10   specific activities authorized under such pilot

11   program;

12   (E) consult with the relevant offices at the

13   Department of Defense that were responsible

14   for launching the 2016 "Hack the Pentagon"

15   pilot program and subsequent Department of

16   Defense bug bounty programs;

17   (F) develop a process by which an ap-

18   proved individual, organization, or company can

19   register with the entity referred to in subpara-

20   graph (B), submit to a background check as de-

21   termined by the Department, and receive a de-

22   termination as to eligibility for participation in

23   such pilot program;

24   (G) engage qualified interested persons, in-

25   cluding nongovernmental sector representatives,

1   about the structure of such pilot program as

2   constructive and to the extent practicable; and

3   (H) consult with relevant United States

4   Government officials to ensure that such pilot

5   program complements persistent network and

6   vulnerability scans of the Department of State's

7   internet-accessible systems, such as the scans

8   conducted pursuant to Binding Operational Di-

9   rective BOD–15–01.

10   (3) DURATION.—The pilot program established

11   under paragraph (1) should be short-term in dura-

12   tion and not last longer than one year.

13   (b) REPORT.—Not later than 180 days after the date

14 on which the bug bounty pilot program under subsection

15 (a) is completed, the Secretary shall submit to the Com-

16 mittee on Foreign Relations of the Senate and the Com-

17 mittee on Foreign Affairs of the House of Representatives

18 a report on such pilot program, including information re-

19 lating to—

20   (1) the number of approved individuals, organi-

21   zations, or companies involved in such pilot pro-

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

23   viduals, organizations, or companies that—

24   (A) registered;

25   (B) were approved;

1   (C) submitted security vulnerabilities; and

2   (D) received compensation;

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

4 the National Vulnerabilities Database of the Na-

5 tional Institute of Standards and Technology, of se-

6 curity vulnerabilities reported as part of such pilot

7 program;

8   (3) the number of previously unidentified secu-

9 rity vulnerabilities remediated as a result of such

10 pilot program;

11   (4) the current number of outstanding pre-

12 viously unidentified security vulnerabilities and De-

13 partment remediation plans;

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

15 porting of security vulnerabilities and remediation of

16 such vulnerabilities;

17   (6) the types of compensation provided under

18 such pilot program; and

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

20 gram.

Passed the House of Representatives January 22, 2019.

Attest:

Clerk.

H. R. 328

AN ACT

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.