116TH CONGRESS
1ST SESSION

S. 1808

To require the Secretary of State to design and establish a Vulnerability Disclosure Process 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 SENATE OF THE UNITED STATES

JUNE 12, 2019

Mr. GARDNER (for himself and Mr. MARKEY) introduced the following bill; which was read twice and referred to the Committee on Foreign Relations

---

A BILL

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

SEC. 2. DEFINITIONS.

In this Act:

(1) BUG BOUNTY PROGRAM.—The term "bug bounty program" means a program under which an approved individual, organization, or company is temporarily authorized to identify and report vulnerabilities of Internet-facing information technology of the Department in exchange for compensation.

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

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

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

(5) VDP.—The term "VDP" means the Vulnerability Disclosure Process established pursuant to section 3.

SEC. 3. DEPARTMENT OF STATE VULNERABILITY DISCLOSURE 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 to improve cybersecurity within the Department by—

1   (1) providing security researchers with clear

2   guidelines for—

3   (A) conducting vulnerability discovery ac-

4   tivities directed at Department information

5   technology; and

6   (B) submitting discovered security vulnera-

7   bilities to the Department; and

8   (2) creating Department procedures and infra-

9   structure to receive and fix discovered vulnerabili-

10   ties.

11   (b) REQUIREMENTS.—In establishing VDP pursuant

12 to subsection (a), the Secretary shall—

13   (1) identify which Department information

14   technology should be included in the process;

15   (2) determine whether the process should dif-

16   ferentiate among and specify the types of security

17   vulnerabilities that may be targeted;

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

19   ing discovered security vulnerabilities and the form

20   in which such vulnerabilities should be reported;

21   (4) identify which Department offices and posi-

22   tions will be responsible for receiving, prioritizing,

23   and addressing security vulnerability disclosure re-

24   ports;

1   (5) consult with the Attorney General regarding

2   how to ensure that individuals, organizations, and

3   companies that comply with the VDP requirements

4   are protected from prosecution under section 1030

5   of title 18, United States Code, and similar provi-

6   sions of law for specific activities authorized under

7   VDP;

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

9   partment of Defense that were responsible for

10   launching the 2016 Vulnerability Disclosure Pro-

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

12   partment of Defense bug bounty programs;

13   (7) engage qualified interested persons, includ-

14   ing nongovernmental sector representatives, about

15   the structure of VDP, as constructive and to the ex-

16   tent practicable; and

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

18   manage VDP and implement the remediation of dis-

19   covered security vulnerabilities.

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

21   after the establishment of VDP under subsection (a) and

22   annually thereafter for the following 6 years, the Secretary

23   shall submit a report to the Committee on Foreign Rela-

24   tions of the Senate and the Committee on Foreign Affairs

1 of the House of Representatives regarding the establish-
2 ment of VDP, including information relating to—

3   (1) 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 through VDP;

7   (2) the number of previously unidentified secu-
8   rity vulnerabilities remediated as a result of such re-
9   porting;

10   (3) the current number of outstanding pre-
11   viously unidentified security vulnerabilities and the
12   Department's remediation plans to address such
13   vulnerabilities;

14   (4) the average period between the reporting of
15   security vulnerabilities and the remediation of such
16   vulnerabilities;

17   (5) the resources, surge staffing, roles, and re-
18   sponsibilities within the Department used to imple-
19   ment VDP and complete the necessary security vul-
20   nerability remediation; and

21   (6) any other information that the Secretary
22   determines to be relevant.

23 **SEC. 4. DEPARTMENT OF STATE BUG BOUNTY PILOT PRO-**
24   **GRAM.**

25   (a) ESTABLISHMENT OF PILOT PROGRAM.—

1   (1) IN GENERAL.—Not later than 1 year after

2 the date of the enactment of this Act, the Secretary

3 shall establish a Bug Bounty Pilot Program to mini-

4 mize security vulnerabilities of Internet-facing infor-

5 mation technology of the Department.

6   (2) REQUIREMENTS.—In establishing the pilot

7 program under paragraph (1), the Secretary shall—

8   (A) provide compensation for reports of

9 previously unidentified security vulnerabilities

10 within the websites, applications, and other

11 Internet-facing information technology of the

12 Department that are accessible to the public;

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

14 essary, to manage the pilot program and for

15 executing the remediation of security vulnerabil-

16 ities identified pursuant to subparagraph (A);

17   (C) identify which Department information

18 technology should be included in the pilot pro-

19 gram;

20   (D) consult with the Attorney General on

21 how to ensure that individuals, organizations,

22 or companies that comply with the requirements

23 of the pilot program are protected from pros-

24 ecution under section 1030 of title 18, United

25 States Code, and similar provisions of law for

1 specific activities authorized under the pilot

2 program;

3 (E) consult with the relevant offices at the

4 Department of Defense that were responsible

5 for launching the 2016 "Hack the Pentagon"

6 pilot program and subsequent Department of

7 Defense bug bounty programs;

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

9 proved individual, organization, or company

10 can—

11 (i) register with entities referred to in

12 subparagraph (B);

13 (ii) submit to a background check, as

14 determined by the Department; and

15 (iii) receive a determination as to eli-

16 gibility for participation in the pilot pro-

17 gram;

18 (G) engage qualified interested persons, in-

19 cluding nongovernmental sector representatives,

20 about the structure of the pilot program, as

21 constructive and to the extent practicable; and

22 (H) consult with relevant United States

23 Government officials to ensure that the pilot

24 program complements persistent network and

25 vulnerability scans of the Department's Inter-

1 net-accessible systems, such as the scans con-

2 ducted pursuant to Binding Operational Direc-

3 tive 15–01, issued by the Secretary of Home-

4 land Security on May 21, 2015.

5 (3) DURATION.—The pilot program established

6 under paragraph (1) should be terminated not later

7 than 1 year after the date on which it is established.

8 (b) REPORT.—Not later than 180 days after the com-

9 pletion of the Bug Bounty Pilot Program under subsection

10 (a), the Secretary shall submit a report to the Committee

11 on Foreign Relations of the Senate and the Committee

12 on Foreign Affairs of the House of Representatives that

13 describes the pilot program, including information regard-

14 ing—

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

16 zations, or companies involved in the pilot program,

17 broken down by—

18 (A) the number of approved individuals,

19 organizations, or companies that registered for

20 the pilot program;

21 (B) the number of such entities that were

22 approved to participate in the pilot program;

23 (C) the number of such entities that sub-

24 mitted security vulnerabilities under the pilot

25 program; and

1   (D) the number of such entities that re-
2   ceived compensation under the pilot program;

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 under the pilot pro-
7   gram;

8   (3) the number of previously unidentified secu-
9   rity vulnerabilities remediated as a result of the pilot
10   program;

11   (4) the current number of outstanding pre-
12   viously unidentified security vulnerabilities and the
13   Department's plans for remediating such vulnerabili-
14   ties;

15   (5) the average period between the reporting of
16   security vulnerabilities and the remediation of such
17   vulnerabilities;

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

20   (7) the lessons learned from the pilot program.

○