117TH CONGRESS
1ST SESSION **H. R. 3313**

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

MAY 18, 2021

Mr. LIEU (for himself, Ms. SPANBERGER, Mr. PFLUGER, and Ms. TENNEY)
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 De-
partment of State cybersecurity and a bug bounty pro-
gram 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.

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—

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 of all security

25 vulnerabilities reported.

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

13   (6) Any other information the Secretary deter-
14 mines relevant.

15 **SEC. 4. DEPARTMENT OF STATE BUG BOUNTY PILOT PRO-**
16   **GRAM.**

17 (a) ESTABLISHMENT OF PILOT PROGRAM.—

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

23   (2) REQUIREMENTS.—In establishing the pilot
24 program described in paragraph (1), the Secretary
25 shall—

1　　　　　(A) provide compensation for reports of

2　　　previously unidentified security vulnerabilities

3　　　within the websites, applications, and other

4　　　internet-facing information technology of the

5　　　Department that are accessible to the public;

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

7　　　essary, to manage such pilot program and for

8　　　executing the remediation of security vulnerabil-

9　　　ities identified pursuant to subparagraph (A);

10　　　　　(C) identify which Department information

11　　　technology should be included in such pilot pro-

12　　　gram;

13　　　　　(D) consult with the Attorney General on

14　　　how to ensure that individuals, organizations,

15　　　or companies that comply with the requirements

16　　　of such pilot program are protected from pros-

17　　　ecution under section 1030 of title 18, United

18　　　States Code, and similar provisions of law for

19　　　specific activities authorized under such pilot

20　　　program;

21　　　　　(E) consult with the relevant offices at the

22　　　Department of Defense that were responsible

23　　　for launching the 2016 ''Hack the Pentagon''

24　　　pilot program and subsequent Department of

25　　　Defense bug bounty programs;

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

2   proved individual, organization, or company can

3   register with the entity referred to in subpara-

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

5   termined by the Department, and receive a de-

6   termination as to eligibility for participation in

7   such pilot program;

8   (G) engage qualified interested persons, in-

9   cluding nongovernmental sector representatives,

10   about the structure of such pilot program as

11   constructive and to the extent practicable; and

12   (H) consult with relevant United States

13   Government officials to ensure that such pilot

14   program complements persistent network and

15   vulnerability scans of the Department of State's

16   internet-accessible systems, such as the scans

17   conducted pursuant to Binding Operational Di-

18   rective BOD–19–02 or successor Directive.

19   (3) DURATION.—The pilot program established

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

21   tion and not last longer than one year.

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

23 on which the bug bounty pilot program under subsection

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

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

1 mittee on Foreign Affairs of the House of Representatives

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

3 lating to—

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

5   zations, or companies involved in such pilot pro-

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

7   viduals, organizations, or companies that—

8   (A) registered;

9   (B) were approved;

10   (C) submitted security vulnerabilities; and

11   (D) received compensation;

12   (2) the number and severity of all security

13   vulnerabilities reported as part of such pilot pro-

14   gram;

15   (3) the number of previously unidentified secu-

16   rity vulnerabilities remediated as a result of such

17   pilot program;

18   (4) the current number of outstanding pre-

19   viously unidentified security vulnerabilities and De-

20   partment remediation plans;

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

22   porting of security vulnerabilities and remediation of

23   such vulnerabilities;

24   (6) the types of compensation provided under

25   such pilot program; and

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

2   gram.

○