[115HR5433.EH]

....
(Original Signature of Member)

116TH CONGRESS
1ST SESSION

H. R. ____

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

_____

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 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,*

1 **SECTION 1. SHORT TITLE.**

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

3 partment Act".

4 **SEC. 2. DEFINITIONS.**

5 In this Act:

6 (1) BUG BOUNTY PROGRAM.—The term "bug

7 bounty program" means a program under which an

8 approved individual, organization, or company is

9 temporarily authorized to identify and report

10 vulnerabilities of internet-facing information tech-

11 nology of the Department in exchange for compensa-

12 tion.

13 (2) DEPARTMENT.—The term "Department"

14 means the Department of State.

15 (3) INFORMATION TECHNOLOGY.—The term

16 "information technology" has the meaning given

17 such term in section 11101 of title 40, United

18 States Code.

19 (4) SECRETARY.—The term "Secretary" means

20 the Secretary of State.

21 **SEC. 3. DEPARTMENT OF STATE VULNERABILITY DISCLO-**

22 **SURE PROCESS.**

23 (a) IN GENERAL.—Not later than 180 days after the

24 date of the enactment of this Act, the Secretary shall de-

25 sign, establish, and make publicly known a Vulnerability

3

1 Disclosure Process (VDP) to improve Department cyber-
2 security by—

3   (1) providing security researchers with clear
4   guidelines for—

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

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

10   (2) creating Department procedures and infra-
11   structure to receive and fix discovered
12   vulnerabilities.

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

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

17   (2) determine whether the process should dif-
18   ferentiate among and specify the types of security
19   vulnerabilities that may be targeted;

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

23   (4) identify which Department offices and posi-
24   tions will be responsible for receiving, prioritizing,

1 and addressing security vulnerability disclosure re-

2 ports;

3   (5) consult with the Attorney General regarding

4 how to ensure that individuals, organizations, and

5 companies that comply with the requirements of the

6 process are protected from prosecution under section

7 1030 of title 18, United States Code, and similar

8 provisions of law for specific activities authorized

9 under the process;

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

11 partment of Defense that were responsible for

12 launching the 2016 Vulnerability Disclosure Pro-

13 gram, ''Hack the Pentagon'', and subsequent De-

14 partment of Defense bug bounty programs;

15   (7) engage qualified interested persons, includ-

16 ing nongovernmental sector representatives, about

17 the structure of the process as constructive and to

18 the extent practicable; and

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

20 manage the process and implement the remediation

21 of discovered security vulnerabilities.

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

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

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

25 retary of State shall submit to the Committee on Foreign

1 Affairs of the House of Representatives and the Com-
2 mittee on Foreign Relations of the Senate a report on the
3 VDP, including information relating to the following:

4 　　(1) The number and severity, in accordance
5 　　with the National Vulnerabilities Database of the
6 　　National Institute of Standards and Technology, of
7 　　security vulnerabilities reported.

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

10 　　(3) The current number of outstanding pre-
11 　　viously unidentified security vulnerabilities and De-
12 　　partment of State remediation plans.

13 　　(4) The average length of time between the re-
14 　　porting of security vulnerabilities and remediation of
15 　　such vulnerabilities.

16 　　(5) The resources, surge staffing, roles, and re-
17 　　sponsibilities within the Department used to imple-
18 　　ment the VDP and complete security vulnerability
19 　　remediation.

20 　　(6) Any other information the Secretary deter-
21 　　mines relevant.

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

24 　　(a) ESTABLISHMENT OF PILOT PROGRAM.—

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

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

3 retary shall establish a bug bounty pilot program to

4 minimize security vulnerabilities of internet-facing

5 information technology of the Department.

6   (2) REQUIREMENTS.—In establishing the pilot

7 program described in paragraph (1), the Secretary

8 shall—

9   (A) provide compensation for reports of

10 previously unidentified security vulnerabilities

11 within the websites, applications, and other

12 internet-facing information technology of the

13 Department that are accessible to the public;

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

15 essary, to manage such pilot program and for

16 executing the remediation of security

17 vulnerabilities identified pursuant to subpara-

18 graph (A);

19   (C) identify which Department information

20 technology should be included in such pilot pro-

21 gram;

22   (D) consult with the Attorney General on

23 how to ensure that individuals, organizations,

24 or companies that comply with the requirements

25 of such pilot program are protected from pros-

1 ecution under section 1030 of title 18, United
2 States Code, and similar provisions of law for
3 specific activities authorized under such pilot
4 program;

5 (E) consult with the relevant offices at the
6 Department of Defense that were responsible
7 for launching the 2016 ''Hack the Pentagon''
8 pilot program and subsequent Department of
9 Defense bug bounty programs;

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

17 (G) engage qualified interested persons, in-
18 cluding nongovernmental sector representatives,
19 about the structure of such pilot program as
20 constructive and to the extent practicable; and

21 (H) consult with relevant United States
22 Government officials to ensure that such pilot
23 program compliments persistent network and
24 vulnerability scans of the Department of State's
25 internet-accessible systems, such as the scans

1   conducted pursuant to Binding Operational Di-

2   rective BOD-15-01.

3   (3) DURATION.—The pilot program established

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

5   tion and not last longer than one year.

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

7 on which the bug bounty pilot program under subsection

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

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

10 mittee on Foreign Affairs of the House of Representatives

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

12 lating to—

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

14   zations, or companies involved in such pilot pro-

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

16   viduals, organizations, or companies that—

17   (A) registered;

18   (B) were approved;

19   (C) submitted security vulnerabilities; and

20   (D) received compensation;

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

22   the National Vulnerabilities Database of the Na-

23   tional Institute of Standards and Technology, of se-

24   curity vulnerabilities reported as part of such pilot

25   program;

1   (3) the number of previously unidentified secu-

2 rity vulnerabilities remediated as a result of such

3 pilot program;

4   (4) the current number of outstanding pre-

5 viously unidentified security vulnerabilities and De-

6 partment remediation plans;

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

8 porting of security vulnerabilities and remediation of

9 such vulnerabilities;

10   (6) the types of compensation provided under

11 such pilot program; and

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

13 gram.