

115TH CONGRESS
2D SESSION

H. R. 5433

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.

1 **SEC. 3. DEPARTMENT OF STATE VULNERABILITY DISCLO-**
2 **SURE PROCESS.**

3 (a) IN GENERAL.—Not later than 180 days after the
4 date of the enactment of this Act, the Secretary shall de-
5 sign, establish, and make publicly known a Vulnerability
6 Disclosure Process (VDP) to improve Department cyber-
7 security by—

8 (1) providing security researchers with clear
9 guidelines for—

10 (A) conducting vulnerability discovery ac-
11 tivities directed at Department information
12 technology; and

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

15 (2) creating Department procedures and infra-
16 structure to receive and fix discovered
17 vulnerabilities.

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

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

22 (2) determine whether the process should dif-
23 ferentiate among and specify the types of security
24 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 approved individuals, organiza-
10 tions, and companies that comply with the require-
11 ments of the process are protected from prosecution
12 under section 1030 of title 18, United States Code,
13 and similar provisions of law for specific activities
14 authorized 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 a contract to an entity, as necessary,
2 to manage the process and implement the remedi-
3 ation 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 following with respect to the VDP:

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) An estimate of the total cost savings of dis-
24 covering and addressing security vulnerabilities sub-
25 mitted through the VDP.

1 (6) The resources, surge staffing, roles, and re-
2 responsibilities within the Department used to imple-
3 ment the VDP and complete security vulnerability
4 remediation.

5 (7) Any other information the Secretary deter-
6 mines relevant.

7 **SEC. 4. DEPARTMENT OF STATE BUG BOUNTY PILOT PRO-**
8 **GRAM.**

9 (a) ESTABLISHMENT OF PILOT PROGRAM.—

10 (1) IN GENERAL.—Not later than one year
11 after the date of the enactment of this Act, the Sec-
12 retary shall establish a bug bounty pilot program to
13 minimize security vulnerabilities of internet-facing
14 information technology of the Department.

15 (2) REQUIREMENTS.—In establishing the pilot
16 program described in paragraph (1), the Secretary
17 shall—

18 (A) provide compensation for reports of
19 previously unidentified security vulnerabilities
20 within the websites, applications, and other
21 internet-facing information technology of the
22 Department that are accessible to the public;

23 (B) award a contract to an entity, as nec-
24 essary, to manage such pilot program and for
25 executing the remediation of security

1 vulnerabilities identified pursuant to subpara-
2 graph (A);

3 (C) identify which Department information
4 technology should be included in such pilot pro-
5 gram;

6 (D) consult with the Attorney General on
7 how to ensure that approved individuals, orga-
8 nizations, or companies that comply with the
9 requirements of such pilot program are pro-
10 tected from prosecution under section 1030 of
11 title 18, United States Code, and similar provi-
12 sions of law for specific activities authorized
13 under such pilot program;

14 (E) consult with the relevant offices at the
15 Department of Defense that were responsible
16 for launching the 2016 “Hack the Pentagon”
17 pilot program and subsequent Department of
18 Defense bug bounty programs;

19 (F) develop a process by which an ap-
20 proved individual, organization, or company can
21 register with the entity referred to in subpara-
22 graph (B), submit to a background check as de-
23 termined by the Department, and receive a de-
24 termination as to eligibility for participation in
25 such pilot program;

1 (G) engage qualified interested persons, in-
2 cluding nongovernmental sector representatives,
3 about the structure of such pilot program as
4 constructive and to the extent practicable; and

5 (H) consult with relevant United States
6 Government officials to ensure that such pilot
7 program compliments persistent network and
8 vulnerability scans of the Department of State's
9 internet-accessible systems, such as the scans
10 conducted pursuant to Binding Operational Di-
11 rective BOD-15-01.

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

15 (b) REPORT.—Not later than 180 days after the date
16 on which the bug bounty pilot program under subsection
17 (a) is completed, the Secretary shall submit to the Com-
18 mittee on Foreign Relations of the Senate and the Com-
19 mittee on Foreign Affairs of the House of Representatives
20 a report on such pilot program, including information re-
21 lating to—

22 (1) the number of approved individuals, organi-
23 zations, or companies involved in such pilot pro-
24 gram, broken down by the number of approved indi-
25 viduals, organizations, or companies that—

1 (A) registered;

2 (B) were approved;

3 (C) submitted security vulnerabilities; and

4 (D) received compensation;

5 (2) the number and severity, in accordance with
6 the National Vulnerabilities Database of the Na-
7 tional Institute of Standards and Technology, of se-
8 curity vulnerabilities reported as part of such pilot
9 program;

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

13 (4) the current number of outstanding pre-
14 viously unidentified security vulnerabilities and De-
15 partment remediation plans;

16 (5) the average length of time between the re-
17 porting of security vulnerabilities and remediation of
18 such vulnerabilities;

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

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

 Passed the House of Representatives September 25,
2018.

Attest:

Clerk.

115TH CONGRESS
2^D SESSION

H. R. 5433

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.