

AMENDMENT NO. _____ Calendar No. _____

Purpose: To establish a bug bounty pilot program within the Department of Homeland Security, and for other purposes.

IN THE SENATE OF THE UNITED STATES—115th Cong., 2d Sess.

H. R. 2825

To amend the Homeland Security Act of 2002 to make certain improvements in the laws administered by the Secretary of Homeland Security, and for other purposes.

Referred to the Committee on _____ and
ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT intended to be proposed by _____

Viz:

1 At the end of subtitle B of title I, insert the following:

2 **SEC. 1134. HACK DHS BUG BOUNTY PILOT PROGRAM.**

3 (a) DEFINITIONS.—In this section:

4 (1) BUG BOUNTY PROGRAM.—The term “bug
5 bounty program” means a program under which an
6 approved individual, organization, or company is
7 temporarily authorized to identify and report
8 vulnerabilities of Internet-facing information tech-
9 nology of the Department in exchange for compensa-
10 tion.

1 (2) DEPARTMENT.—The term “Department”
2 means the Department of Homeland Security.

3 (3) INFORMATION TECHNOLOGY.—The term
4 “information technology” has the meaning given the
5 term in section 11101 of title 40, United States
6 Code.

7 (4) PILOT PROGRAM.—The term “pilot pro-
8 gram” means the bug bounty pilot program required
9 to be established under subsection (b)(1).

10 (5) SECRETARY.—The term “Secretary” means
11 the Secretary of Homeland Security.

12 (b) ESTABLISHMENT OF PILOT PROGRAM.—

13 (1) IN GENERAL.—Not later than 180 days
14 after the date of enactment of this Act, the Sec-
15 retary shall establish, within the Office of the Chief
16 Information Officer, a bug bounty pilot program to
17 minimize vulnerabilities of Internet-facing informa-
18 tion technology of the Department.

19 (2) REQUIREMENTS.—In establishing the pilot
20 program, the Secretary shall—

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

1 (B) award a competitive contract to an en-
2 tity, as necessary, to manage the pilot program
3 and for executing the remediation of
4 vulnerabilities identified as a consequence of the
5 pilot program;

6 (C) designate mission-critical operations
7 within the Department that should be excluded
8 from the pilot program;

9 (D) consult with the Attorney General on
10 how to ensure that approved individuals, orga-
11 nizations, or companies that comply with the
12 requirements of the pilot program are protected
13 from prosecution under section 1030 of title 18,
14 United States Code, and similar provisions of
15 law for specific activities authorized under the
16 pilot program;

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

22 (F) develop an expeditious process by
23 which an approved individual, organization, or
24 company can register with the entity described
25 in subparagraph (B), submit to a background

1 check as determined by the Department, and
2 receive a determination as to eligibility for par-
3 ticipation in the pilot program; and

4 (G) engage qualified interested persons, in-
5 cluding non-government sector representatives,
6 about the structure of the pilot program as con-
7 structive and to the extent practicable.

8 (c) REPORT.—Not later than 180 days after the date
9 on which the pilot program is completed, the Secretary
10 shall submit to the Committee on Homeland Security and
11 Governmental Affairs of the Senate and the Committee
12 on Homeland Security of the House of Representatives a
13 report on the pilot program, which shall include—

14 (1) the number of approved individuals, organi-
15 zations, or companies involved in the pilot program,
16 broken down by the number of approved individuals,
17 organizations, or companies that—

18 (A) registered;

19 (B) were approved;

20 (C) submitted security vulnerabilities; and

21 (D) received compensation;

22 (2) the number and severity of vulnerabilities
23 reported as part of the pilot program;

1 (3) the number of previously unidentified secu-
2 rity vulnerabilities remediated as a result of the pilot
3 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 the vulnerabilities;

10 (6) the types of compensation provided under
11 the pilot program; and

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

13 (d) AUTHORIZATION OF APPROPRIATIONS.—There
14 are authorized to be appropriated to the Department
15 \$250,000 for fiscal year 2018 to carry out this section.