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


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:

SEC. 1134. HACK DHS BUG BOUNTY PILOT PROGRAM.

(a) DEFINITIONS.—In this section:

(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 Homeland Security.

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

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

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

(b) ESTABLISHMENT OF PILOT PROGRAM.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Secretary shall establish, within the Office of the Chief Information Officer, a bug bounty pilot program to minimize vulnerabilities of Internet-facing information technology of the Department.

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

(A) provide compensation for reports of previously unidentified security vulnerabilities within the websites, applications, and other Internet-facing information technology of the Department that are accessible to the public;
(B) award a competitive contract to an entity, as necessary, to manage the pilot program and for executing the remediation of vulnerabilities identified as a consequence of the pilot program;

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

(D) consult with the Attorney General on how to ensure that approved individuals, organizations, or companies that comply with the requirements of the pilot program are protected from prosecution under section 1030 of title 18, United States Code, and similar provisions of law for specific activities authorized under the pilot program;

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

(F) develop an expeditious process by which an approved individual, organization, or company can register with the entity described in subparagraph (B), submit to a background
check as determined by the Department, and receive a determination as to eligibility for participation in the pilot program; and

(G) engage qualified interested persons, including non-government sector representatives, about the structure of the pilot program as constructive and to the extent practicable.

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

(1) the number of approved individuals, organizations, or companies involved in the pilot program, broken down by the number of approved individuals, organizations, or companies that—

(A) registered;

(B) were approved;

(C) submitted security vulnerabilities; and

(D) received compensation;

(2) the number and severity of vulnerabilities reported as part of the pilot program;
(3) the number of previously unidentified security vulnerabilities remediated as a result of the pilot program;

(4) the current number of outstanding previously unidentified security vulnerabilities and Department remediation plans;

(5) the average length of time between the reporting of security vulnerabilities and remediation of the vulnerabilities;

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

(7) the lessons learned from the pilot program.

(d) Authorization of Appropriations.—There are authorized to be appropriated to the Department $250,000 for fiscal year 2018 to carry out this section.