

.....
(Original Signature of Member)

115TH CONGRESS
2D SESSION

H. R. 6735

To direct the Secretary of Homeland Security to establish a vulnerability disclosure policy for Department of Homeland Security internet websites, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

M____ introduced the following bill; which was referred to the
Committee on _____

A BILL

To direct the Secretary of Homeland Security to establish a vulnerability disclosure policy for Department of Homeland Security internet websites, 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. DEPARTMENT OF HOMELAND SECURITY DIS-**
4 **CLOSURE OF SECURITY VULNERABILITIES.**

5 (a) VULNERABILITY DISCLOSURE POLICY.—The Sec-
6 retary of Homeland Security shall establish a policy appli-
7 cable to individuals, organizations, and companies that re-

1 port security vulnerabilities on Department of Homeland
2 Security public internet websites that shall include:

3 (1) the information technology to which the pol-
4 icy applies;

5 (2) the conditions under which parties may le-
6 gally operate to discover and report security
7 vulnerabilities;

8 (3) how individuals, organizations, and compa-
9 nies should disclose discovered security
10 vulnerabilities to the Department;

11 (4) the communication that parties that report
12 security vulnerabilities should expect from the De-
13 partment; and

14 (5) how the Department will disclose, or how
15 parties that report security vulnerabilities may dis-
16 close, reported security vulnerabilities.

17 (b) REMEDIATION PROCESS.—The Secretary shall
18 develop a process for the Department of Homeland Secu-
19 rity to address how the Department will mitigate or reme-
20 diate security vulnerabilities reported through the policy
21 developed in subsection (a).

22 (c) CONSULTATION.—In developing the security vul-
23 nerability disclosure policy under subsection (a), the Sec-
24 retary shall consult with

1 (1) the Attorney General regarding how to en-
2 sure that individuals, organizations, and companies
3 that comply with the requirements of the policy de-
4 veloped under subsection (a) are protected from
5 prosecution under section 1030 of title 18, United
6 States Code, civil lawsuits, and similar provisions of
7 law with respect to specific activities authorized
8 under the policy;

9 (2) the Secretary of Defense and the Adminis-
10 trator of General Services regarding lessons that
11 may be applied from existing vulnerability disclosure
12 programs; and

13 (3) non-governmental security researchers.

14 (d) PUBLIC AVAILABILITY.—The Secretary shall
15 make the policy developed under subsection (a) publicly
16 available.

17 (e) SUBMISSION TO CONGRESS.—

18 (1) Not later than 90 days after the date of the
19 enactment of this Act, the Secretary shall submit to
20 Congress the policy required under subsection (a)
21 and the remediation process required under sub-
22 section (b).

23 (2) Not later than one year after creating the
24 policy required under subsection (a) the Secretary
25 shall submit a report to Congress, and annually

1 thereafter for each of the next three years, the Sec-
2 retary shall brief Congress with the following infor-
3 mation with respect to the policy required under
4 subsection (a) and the process required under sub-
5 section (b):

6 (A) the number of unique security
7 vulnerabilities reported,

8 (B) the number of previously unknown se-
9 curity vulnerabilities mitigated or remediated,

10 (C) the number of unique parties that re-
11 ported security vulnerabilities, and

12 (D) the average length of time between the
13 reporting of security vulnerabilities and mitiga-
14 tion or remediation of such vulnerabilities.

15 (f) DEFINITIONS.—In this section,

16 (1) the term “security vulnerability” has the
17 meaning given that term in section 1501 of title 6,
18 United States Code, in information technology.

19 (2) the term “information system” has the
20 meaning given that term by section 3502 of title 44,
21 United States Code.