

115TH CONGRESS
2D SESSION

S. 3707

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 SENATE OF THE UNITED STATES

DECEMBER 5, 2018

Mr. PORTMAN (for himself and Ms. HASSAN) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

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. SHORT TITLE.**

4 This Act may be cited as the “Public-Private Cyber-
5 security Cooperation Act”.

6 **SEC. 2. DEPARTMENT OF HOMELAND SECURITY DISCLO-**
7 **SURE OF SECURITY VULNERABILITIES.**

8 (a) DEFINITIONS.—In this section:

1 (1) APPROPRIATE INFORMATION SYSTEM.—The
2 term “appropriate information system” means an in-
3 formation system that the Secretary of Homeland
4 Security selects for inclusion under the vulnerability
5 disclosure policy required by subsection (b).

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

8 (3) INFORMATION SYSTEM.—The term “infor-
9 mation system” has the meaning given that term by
10 section 3502(12) of title 44, United States Code.

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

13 (5) SECURITY VULNERABILITY.—The term “se-
14 curity vulnerability” has the meaning given that
15 term in section 102(17) of the Cybersecurity Infor-
16 mation Sharing Act of 2015 (6 U.S.C. 1501(17)), in
17 information technology.

18 (b) VULNERABILITY DISCLOSURE POLICY.—The Sec-
19 retary shall establish a policy applicable to individuals, or-
20 ganizations, and companies that report security vulnera-
21 bilities on appropriate information systems of Depart-
22 ment. Such policy shall include each of the following:

23 (1) The appropriate information systems of the
24 Department that individuals, organizations, and

1 companies may use to discover and report security
2 vulnerabilities on appropriate information systems.

3 (2) The conditions and criteria under which in-
4 dividuals, organizations, and companies may operate
5 to discover and report security vulnerabilities.

6 (3) How individuals, organizations, and compa-
7 nies may disclose to the Department security vulner-
8 abilities discovered on appropriate information sys-
9 tems of the Department.

10 (4) The ways in which the Department may
11 communicate with individuals, organizations, and
12 companies that report security vulnerabilities.

13 (5) The process the Department shall use for
14 public disclosure of reported security vulnerabilities.

15 (c) REMEDIATION PROCESS.—The Secretary shall
16 develop a process for the Department to address the miti-
17 gation or remediation of the security vulnerabilities re-
18 ported through the policy developed in subsection (b).

19 (d) CONSULTATION.—

20 (1) IN GENERAL.—In developing the security
21 vulnerability disclosure policy under subsection (b),
22 the Secretary shall consult with each of the fol-
23 lowing:

24 (A) The Attorney General regarding how
25 to ensure that individuals, organizations, and

1 companies that comply with the requirements of
2 the policy developed under subsection (b) are
3 protected from prosecution under section 1030
4 of title 18, United States Code, civil lawsuits,
5 and similar provisions of law with respect to
6 specific activities authorized under the policy.

7 (B) The Secretary of Defense and the Ad-
8 ministrator of General Services regarding les-
9 sons that may be applied from existing vulner-
10 ability disclosure policies.

11 (C) Non-governmental security researchers.

12 (2) NONAPPLICABILITY OF FACA.—The Federal
13 Advisory Committee Act (5 U.S.C. App.) shall not
14 apply to any consultation under this section.

15 (e) PUBLIC AVAILABILITY.—The Secretary shall
16 make the policy developed under subsection (b) publicly
17 available.

18 (f) SUBMISSION TO CONGRESS.—

19 (1) DISCLOSURE POLICY AND REMEDIATION
20 PROCESS.—Not later than 90 days after the date of
21 enactment of this Act, the Secretary shall submit to
22 Congress a copy of the policy required under sub-
23 section (b) and the remediation process required
24 under subsection (c).

25 (2) REPORT AND BRIEFING.—

1 (A) REPORT.—Not later than 1 year after
2 establishing the policy required under sub-
3 section (b), the Secretary shall submit to Con-
4 gress a report on such policy and the remedi-
5 ation process required under subsection (c).

6 (B) ANNUAL BRIEFINGS.—One year after
7 the date of the submission of the report under
8 subparagraph (A), and annually thereafter for
9 each of the next 3 years, the Secretary shall
10 provide to Congress a briefing on the policy re-
11 quired under subsection (b) and the process re-
12 quired under subsection (c).

13 (C) MATTERS FOR INCLUSION.—The re-
14 port required under subparagraph (A) and the
15 briefings required under subparagraph (B) shall
16 include each of the following with respect to the
17 policy required under subsection (b) and the
18 process required under subsection (c) for the
19 period covered by the report or briefing, as the
20 case may be:

21 (i) The number of unique security
22 vulnerabilities reported.

23 (ii) The number of previously un-
24 known security vulnerabilities mitigated or
25 remediated.

1 (iii) The number of unique individ-
2 uals, organizations, and companies that re-
3 ported security vulnerabilities.

4 (iv) The average length of time be-
5 tween the reporting of security vulnerabili-
6 ties and mitigation or remediation of such
7 vulnerabilities.

○