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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Public-Private Cybersecurity Cooperation Act''.

SEC. 2. DEPARTMENT OF HOMELAND SECURITY DISCLOSURE OF SECURITY VULNERABILITIES.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE INFORMATION SYSTEM.—The term ''appropriate information system'' means an information system that the Secretary of Homeland Security selects for inclusion under the vulnerability disclosure policy required by subsection (b).

(2) DEPARTMENT.—The term ''Department'' means the Department of Homeland Security.

(3) INFORMATION SYSTEM.—The term ''information system'' has the meaning given that term by section 3502(12) of title 44, United States Code.

(4) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

(5) SECURITY VULNERABILITY.—The term ''security vulnerability'' has the meaning given that term in section 102(17) of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501(17)), in information technology.

(b) VULNERABILITY DISCLOSURE POLICY.—The Secretary shall establish a policy applicable to individuals, organizations, and companies that report security vulnerabilities on appropriate information systems of Department. Such policy shall include each of the following:

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

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

(2) The conditions and criteria under which individuals, organizations, and companies may operate to discover and report security vulnerabilities.

(3) How individuals, organizations, and companies may disclose to the Department security vulnerabilities discovered on appropriate information systems of the Department.

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

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

(c) REMEDIATION PROCESS.—The Secretary shall develop a process for the Department to address the mitigation or remediation of the security vulnerabilities reported through the policy developed in subsection (b).

(d) CONSULTATION.—

(1) IN GENERAL.—In developing the security vulnerability disclosure policy under subsection (b), the Secretary shall consult with each of the following:

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

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

(B) The Secretary of Defense and the Administrator of General Services regarding lessons that may be applied from existing vulnerability disclosure policies.

(C) Non-governmental security researchers.

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

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

(f) SUBMISSION TO CONGRESS.—

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

(2) REPORT AND BRIEFING.—

(A) REPORT.—Not later than 1 year after establishing the policy required under subsection (b), the Secretary shall submit to Congress a report on such policy and the remediation process required under subsection (c).

(B) ANNUAL BRIEFINGS.—One year after the date of the submission of the report under subparagraph (A), and annually thereafter for each of the next 3 years, the Secretary shall provide to Congress a briefing on the policy required under subsection (b) and the process required under subsection (c).

(C) MATTERS FOR INCLUSION.—The report required under subparagraph (A) and the briefings required under subparagraph (B) shall include each of the following with respect to the policy required under subsection (b) and the process required under subsection (c) for the period covered by the report or briefing, as the case may be:

(i) The number of unique security vulnerabilities reported.

(ii) The number of previously unknown security vulnerabilities mitigated or remediated.

(iii) The number of unique individuals, organizations, and companies that reported security vulnerabilities.

(iv) The average length of time between the reporting of security vulnerabilities and mitigation or remediation of such vulnerabilities.

○