To direct the Secretary of Homeland Security to establish a vulnerability disclosure policy for Department of Homeland Security internet websites, and for other purposes.
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 Representa-
tives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “Public-Private Cyberse-
curity Cooperation Act”.

SEC. 2. DEPARTMENT OF HOMELAND SECURITY DISCLO-
SURE OF SECURITY VULNERABILITIES.

(a) VULNERABILITY DISCLOSURE POLICY.—The Sec-
retary of Homeland Security shall establish a policy applic-
cable to individuals, organizations, and companies that re-
port security vulnerabilities on appropriate information
systems of Department of Homeland Security. Such policy
shall include each of the following:

(1) The appropriate information systems of the
Department that individuals, organizations, and com-
panies may use to discover and report security
vulnerabilities on appropriate information systems.

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

(3) How individuals, organizations, and compa-
nies 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.

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

(c) CONSULTATION.—In developing the security vulnerability disclosure policy under subsection (a), the Secretary of Homeland Security shall consult with each of the following:

(1) The Attorney General regarding how to ensure that individuals, organizations, and companies that comply with the requirements of the policy developed under subsection (a) 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.

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

(3) Non-governmental security researchers.

(d) **Public Availability.**—The Secretary of Homeland Security shall make the policy developed under subsection (a) publicly available.

(e) **Submission to Congress.**—

(1) **Disclosure Policy and Remediation Process.**—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to Congress a copy of the policy required under subsection (a) and the remediation process required under subsection (b).

(2) **Report and Briefing.**—

(A) **Report.**—Not later than one year after establishing the policy required under subsection (a), the Secretary of Homeland Security shall submit to Congress a report on such policy and the remediation process required under subsection (b).

(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 three years, the Secretary of Homeland Security shall provide to Congress a
briefing on the policy required under subsection (a) and the process required under subsection (b).

(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 (a) and the process required under subsection (b) 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.

(f) DEFINITIONS.—In this section:
(1) 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.

(2) The term “information system” has the meaning given that term by section 3502(12) of title 44, United States Code.

(3) 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 (a).