115TH CONGRESS
1ST SESSION

S. _____

To establish the Vulnerability Equities Review Board, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. SCHATZ (for himself, Mr. JOHNSON, and Mr. GARDNER) introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To establish the Vulnerability Equities Review Board, 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 "Protecting Our Ability to Counter Hacking Act of 2017" or "PATCH Act of 2017".

SEC. 2. VULNERABILITY EQUITIES REVIEW BOARD.

(a) DEFINITIONS.—In this section:

(1) FEDERAL AGENCY.—The term ''Federal agency'' has the meaning given such term in section 551 of title 5, United States Code.

(2) PUBLICLY KNOWN.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term ''publicly known'', with respect to information regarding a vulnerability, means information that—

(i) is—

(I) a verbal or electronic presentation or discussion in a publicly accessible domain; or

(II) in a paper or other published documentation in the public domain; and

(ii) that specifically discusses the vulnerability and how the vulnerability could be exploited.

(B) CLASSIFIED MATERIAL.—Information about a vulnerability shall not be considered ''publicly known'' if the information is currently protected as classified and has been inappropriately released to the public.

(3) VENDOR.—The term ''vendor'', with respect to a technology, product, system, service, or application, means the person who—

(A) developed the technology, product, system, service, or application; or

(B) is responsible for maintaining the technology, product, system, service, or application.

(4) VULNERABILITY.—The term ''vulnerability'' means a design, configuration, or implementation weakness in a technology, product, system, service, or application that can be exploited or triggered to cause unexpected or unintended behavior.

(b) ESTABLISHMENT.—There is established the Vulnerability Equities Review Board (in this section the ''Board'').

(c) MEMBERSHIP.—

(1) PERMANENT MEMBERS.—The permanent members of the Board consist of the following:

(A) The Secretary of Homeland Security, or the designee of the Secretary, who shall be the chair of the Board.

(B) The Director of the Federal Bureau of Investigation, or the designee of the Director.

(C) The Director of National Intelligence, or the designee of the Director.

(D) The Director of the Central Intelligence Agency, or the designee of the Director.

(E) The Director of the National Security Agency, or the designee of the Director.

(F) The Secretary of Commerce, or the designee of the Secretary.

(2) AD HOC MEMBERS.—The Board shall include as members, on an ad hoc basis, the following:

(A) The Secretary of State, or the designee of the Secretary, when the Board considers matters under the jurisdiction of such secretary.

(B) The Secretary of the Treasury, or the designee of the Secretary, when the Board considers matters under the jurisdiction of such secretary.

(C) The Secretary of Energy, or the designee of the Secretary, when the Board considers matters under the jurisdiction of such secretary.

(D) The Federal Trade Commission, or the designee of the Commission, when the Board considers matters relating to the Commission.

(3) OTHER PARTICIPANTS.—Any member of the National Security Council under section 101 of the

National Security Act of 1947 (50 U.S.C. 3021) who is not a permanent or ad hoc member of the Board may, with the approval of the President, participate in activities of the Board when requested by the Board.

(d) DUTIES.—

(1) POLICIES.—

(A) IN GENERAL.—The Board shall establish policies on matters relating to whether, when, how, to whom, and to what degree information about a vulnerability that is not publicly known should be shared or released by the Federal Government to a non-Federal entity.

(B) AVAILABILITY TO THE PUBLIC.—To the degree that the policies established under subparagraph (A) are unclassified, the Board shall make such policies available to the public.

(C) DRAFT POLICIES.—

(i) SUBMITTAL TO CONGRESS.—

(I) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Board shall submit to Congress and the President a draft of the policies required by subparagraph (A), along with a descrip-

tion of any challenges or impediments that may require legislative or administrative action.

(II) FORM.—The draft submitted under subclause (I) shall be in unclassified form, but may include a classified annex.

(ii) PUBLICATION.—Not later than 240 days after the date of the enactment of this Act, the Board shall make available to the public a draft of the policies required by subparagraph (A), to the degree that such policies are unclassified.

(2) REQUIREMENT.—The head of each Federal agency shall, upon obtaining information about a vulnerability that is not publicly known, subject such information to the process established under paragraph (3)(A).

(3) PROCESS.—

(A) IN GENERAL.—The Board shall establish the process by which the Board determines whether, when, how, to whom, and to what degree the Federal Government shares or releases information to a non-Federal entity about a vulnerability that is not publicly known.

(B) CONSIDERATIONS.—The process established under subparagraph (A) shall include, with respect to a vulnerability, consideration of the following:

(i) Which technologies, products, systems, services, or applications are subject to the vulnerability, including whether the products or systems are used in core Internet infrastructure, in other critical infrastructure systems, in the United States economy, or in national security systems.

(ii) The potential risks of leaving the vulnerability unpatched or unmitigated.

(iii) The harm that could occur if an actor, such as an adversary of the United States or a criminal organization, were to obtain information about the vulnerability.

(iv) How likely it is that the Federal Government would know if someone external to the Federal Government were exploiting the vulnerability.

(v) The need of the Federal Government to exploit the vulnerability.

(vi) Whether the vulnerability is needed for a specific ongoing intelligence or national security operation.

(vii) If a Federal entity would like to exploit the vulnerability to obtain information, whether there are other means available to the Federal entity to obtain such information.

(viii) The likelihood that a non-Federal entity will discover the vulnerability.

(ix) The risks to foreign countries and the people of foreign countries of not sharing or releasing information about the vulnerability.

(x) Whether the vulnerability can be patched or otherwise mitigated.

(xi) Whether the affected non-Federal entity has a publicly disclosed policy for reporting and disclosing vulnerabilities.

(4) EXCLUSION FROM PROCESS OF VULNERABILITIES PRESUMPTIVELY SHAREABLE OR RELEASABLE.—

(A) IN GENERAL.—Under guidelines established by the Board, a Federal agency may share or release information to a non-Federal

entity about a vulnerability without subjecting such information to the process under paragraph (3)(A) if the agency determines that such information is presumptively shareable or releasable. The guidelines shall specify the standards to be used to determine whether or not information is presumptively shareable or releasable for purposes of this paragraph.

(B) RULE OF CONSTRUCTION.—Subparagraph (A) shall not be construed to imply that information which is determined under such subparagraph to be presumptively shareable or releasable is exempt from the requirements of subparagraph (A) of paragraph (5) or the sharing process established under subparagraph (B) of such paragraph.

(5) DISSEMINATION OF INFORMATION ON VULNERABILITIES.—

(A) SHARING THROUGH SECRETARY OF HOMELAND SECURITY.—

(i) IN GENERAL.—In any case in which the Board determines under paragraph (3)(A) that information about a vulnerability not otherwise publicly known should be shared with or released to an ap-

propriate vendor, the Board shall provide the information to the Secretary of Homeland Security and the Secretary shall, on behalf of the Federal Government, share or release the information as directed by the Board.

(ii) PRESUMPTIVELY SHAREABLE OR RELEASABLE INFORMATION.—In any case in which a Federal agency determines under paragraph (4)(A) that information about a vulnerability is presumptively shareable or releasable, the Federal agency shall provide such information to the Secretary and the Secretary shall, on behalf of the Federal Government, share or release the information.

(B) SHARING PROCESS.—

(i) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security, in coordination with the Secretary of Commerce, shall establish the process by which the Secretary of Homeland Security shares or releases information pursuant to subparagraph (A).

(ii) USE OF VOLUNTARY CONSENSUS STANDARDS.—The Secretary shall ensure that

(I) any sharing or release of information under subparagraph (A) is made in accordance with voluntary consensus standards for disclosure of vulnerabilities; and

(II) the process established under clause (i) is consistent with such standards.

(C) INFORMATION NOT DETERMINED TO BE SHAREABLE OR RELEASABLE.—

(i) IN GENERAL.—The policies under paragraph (1) shall provide for—

(I) the periodic review of vulnerabilities that are determined by the Board, pursuant to the process established under paragraph (3)(A), not to be shareable or releasable, in order to determine whether such vulnerabilities may be shared or released in a manner consistent with the national security interests of the United States; and

(II) the sharing with or releasing to appropriate non-Federal entities of information about vulnerabilities that may be shared or released in a manner consistent with the national security interests of the United States following review under subclause (I).

(ii) IN CASE OF LATER BECOMING PUBLICLY KNOWN.—

(I) IN GENERAL.—In the case of a vulnerability that was not publicly known and determined not to be shareable or releasable pursuant to clause (i)(I) and then subsequently becomes publicly known, the vulnerability shall not be subject to the process established under paragraph (3)(A) and shall be subject to such other Federal procedures and interagency operation processes as may be applicable, such as procedures and processes established to carry out the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.).

(II) APPLICABILITY TO CLASSIFIED MATERIAL.—In this clause, subparagraph (B) of subsection (a)(2) shall not apply.

(e) COMPLIANCE.—Each head of a Federal agency shall ensure that the agency complies with the policies issued by the Board under this section.

(f) OVERSIGHT.—

(1) ANNUAL REPORTS BY BOARD.—

(A) IN GENERAL.—Not less frequently than once each year, the Board shall submit to the appropriate committees of Congress a report on the activities of the Board and the policies issued under subsection (d).

(B) CONTENTS.—In addition to information about the activities and policies described in subparagraph (A), the report required by such subparagraph shall also include the following:

(i) The frequency of meetings held by the Board.

(ii) The aggregate number of vulnerabilities reviewed by the Board.

(iii) The number of vulnerabilities determined by the Board to be shareable or releasable.

(iv) The number of vulnerabilities determined by the Board not to be shareable or releasable.

(v) Such other matters as the Board considers appropriate.

(C) AVAILABILITY TO THE PUBLIC.—For each report submitted under subparagraph (A), the Board shall make an unclassified version of the report available to the public.

(2) ANNUAL REPORTS ON ACTIVITIES OF IGS.—

(A) IN GENERAL.—Not less frequently than once each year, the Inspector General of the Department of Homeland Security shall, in consultation with the Inspectors General of other Federal agencies whose work is affected by activities of the Board, submit to the appropriate committees of Congress a report on the activities of all such Inspectors General during the preceding year in connection with the activities of the Board, the policies issued under subsection (d), and the sharing and releasing of in-

formation about vulnerabilities pursuant to such policies.

(B) AVAILABILITY TO THE PUBLIC.—For each report submitted under subparagraph (A), the Inspector General of the Department of Homeland Security shall make an unclassified version of the report available to the public.

(3) FORM.—Each report under paragraphs (1) and (2) shall be submitted in unclassified form, but may include a classified annex.

(4) REVIEW BY PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD.—

(A) IN GENERAL.—The Privacy and Civil Liberties Oversight Board shall review each report submitted under paragraph (1).

(B) CONSULTATION.—The Vulnerability Equities Review Board may consult with the Privacy and Civil Liberties Oversight Board as the Vulnerability Equities Review Board considers appropriate.

(5) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this subsection, the term ''appropriate committees of Congress'' means—

(A) the Committee on Homeland Security and Governmental Affairs, the Committee on

Commerce, Science, and Transportation, and the Select Committee on Intelligence of the Senate; and

(B) the Committee on Homeland Security, the Committee on Oversight and Government Reform, the Committee on Energy and Commerce, and the Permanent Select Committee on Intelligence of the House of Representatives.