

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.

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 “Protecting Our Ability
5 to Counter Hacking Act of 2017” or “PATCH Act of
6 2017”.

7 **SEC. 2. VULNERABILITY EQUITIES REVIEW BOARD.**

8 (a) **DEFINITIONS.**—In this section:

1 (1) FEDERAL AGENCY.—The term “Federal
2 agency” has the meaning given such term in section
3 551 of title 5, United States Code.

4 (2) PUBLICLY KNOWN.—

5 (A) IN GENERAL.—Except as provided in
6 subparagraph (B), the term “publicly known”,
7 with respect to information regarding a vulner-
8 ability, means information that—

9 (i) is—

10 (I) a verbal or electronic presen-
11 tation or discussion in a publicly ac-
12 cessible domain; or

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

16 (ii) that specifically discusses the vul-
17 nerability and how the vulnerability could
18 be exploited.

19 (B) CLASSIFIED MATERIAL.—Information
20 about a vulnerability shall not be considered
21 “publicly known” if the information is currently
22 protected as classified and has been inappropri-
23 ately released to the public.

1 (D) The Director of the Central Intel-
2 ligence Agency, or the designee of the Director.

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

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

7 (2) AD HOC MEMBERS.—The Board shall in-
8 clude as members, on an ad hoc basis, the following:

9 (A) The Secretary of State, or the designee
10 of the Secretary, when the Board considers
11 matters under the jurisdiction of such sec-
12 retary.

13 (B) The Secretary of the Treasury, or the
14 designee of the Secretary, when the Board con-
15 siders matters under the jurisdiction of such
16 secretary.

17 (C) The Secretary of Energy, or the des-
18 ignee of the Secretary, when the Board con-
19 siders matters under the jurisdiction of such
20 secretary.

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

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

1 National Security Act of 1947 (50 U.S.C. 3021)
2 who is not a permanent or ad hoc member of the
3 Board may, with the approval of the President, par-
4 ticipate in activities of the Board when requested by
5 the Board.

6 (d) DUTIES.—

7 (1) POLICIES.—

8 (A) IN GENERAL.—The Board shall estab-
9 lish policies on matters relating to whether,
10 when, how, to whom, and to what degree infor-
11 mation about a vulnerability that is not publicly
12 known should be shared or released by the Fed-
13 eral Government to a non-Federal entity.

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

18 (C) DRAFT POLICIES.—

19 (i) SUBMITTAL TO CONGRESS.—

20 (I) IN GENERAL.—Not later than
21 180 days after the date of the enact-
22 ment of this Act, the Board shall sub-
23 mit to Congress and the President a
24 draft of the policies required by sub-
25 paragraph (A), along with a descrip-

1 tion of any challenges or impediments
2 that may require legislative or admin-
3 istrative action.

4 (II) FORM.—The draft submitted
5 under subclause (I) shall be in unclas-
6 sified form, but may include a classi-
7 fied annex.

8 (ii) PUBLICATION.—Not later than
9 240 days after the date of the enactment
10 of this Act, the Board shall make available
11 to the public a draft of the policies re-
12 quired by subparagraph (A), to the degree
13 that such policies are unclassified.

14 (2) REQUIREMENT.—The head of each Federal
15 agency shall, upon obtaining information about a
16 vulnerability that is not publicly known, subject such
17 information to the process established under para-
18 graph (3)(A).

19 (3) PROCESS.—

20 (A) IN GENERAL.—The Board shall estab-
21 lish the process by which the Board determines
22 whether, when, how, to whom, and to what de-
23 gree the Federal Government shares or releases
24 information to a non-Federal entity about a vul-
25 nerability that is not publicly known.

1 (B) CONSIDERATIONS.—The process estab-
2 lished under subparagraph (A) shall include,
3 with respect to a vulnerability, consideration of
4 the following:

5 (i) Which technologies, products, sys-
6 tems, services, or applications are subject
7 to the vulnerability, including whether the
8 products or systems are used in core Inter-
9 net infrastructure, in other critical infra-
10 structure systems, in the United States
11 economy, or in national security systems.

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

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

18 (iv) How likely it is that the Federal
19 Government would know if someone exter-
20 nal to the Federal Government were ex-
21 ploiting the vulnerability.

22 (v) The need of the Federal Govern-
23 ment to exploit the vulnerability.

1 (vi) Whether the vulnerability is need-
2 ed for a specific ongoing intelligence or na-
3 tional security operation.

4 (vii) If a Federal entity would like to
5 exploit the vulnerability to obtain informa-
6 tion, whether there are other means avail-
7 able to the Federal entity to obtain such
8 information.

9 (viii) The likelihood that a non-Fed-
10 eral entity will discover the vulnerability.

11 (ix) The risks to foreign countries and
12 the people of foreign countries of not shar-
13 ing or releasing information about the vul-
14 nerability.

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

17 (xi) Whether the affected non-Federal
18 entity has a publicly disclosed policy for re-
19 porting and disclosing vulnerabilities.

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

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

1 entity about a vulnerability without subjecting
2 such information to the process under para-
3 graph (3)(A) if the agency determines that such
4 information is presumptively shareable or re-
5 leasable. The guidelines shall specify the stand-
6 ards to be used to determine whether or not in-
7 formation is presumptively shareable or releas-
8 able for purposes of this paragraph.

9 (B) RULE OF CONSTRUCTION.—Subpara-
10 graph (A) shall not be construed to imply that
11 information which is determined under such
12 subparagraph to be presumptively shareable or
13 releasable is exempt from the requirements of
14 subparagraph (A) of paragraph (5) or the shar-
15 ing process established under subparagraph (B)
16 of such paragraph.

17 (5) DISSEMINATION OF INFORMATION ON
18 VULNERABILITIES.—

19 (A) SHARING THROUGH SECRETARY OF
20 HOMELAND SECURITY.—

21 (i) IN GENERAL.—In any case in
22 which the Board determines under para-
23 graph (3)(A) that information about a vul-
24 nerability not otherwise publicly known
25 should be shared with or released to an ap-

1 appropriate vendor, the Board shall provide
2 the information to the Secretary of Home-
3 land Security and the Secretary shall, on
4 behalf of the Federal Government, share or
5 release the information as directed by the
6 Board.

7 (ii) PRESUMPTIVELY SHAREABLE OR
8 RELEASABLE INFORMATION.—In any case
9 in which a Federal agency determines
10 under paragraph (4)(A) that information
11 about a vulnerability is presumptively
12 shareable or releasable, the Federal agency
13 shall provide such information to the Sec-
14 retary and the Secretary shall, on behalf of
15 the Federal Government, share or release
16 the information.

17 (B) SHARING PROCESS.—

18 (i) IN GENERAL.—Not later than 180
19 days after the date of the enactment of
20 this Act, the Secretary of Homeland Secu-
21 rity, in coordination with the Secretary of
22 Commerce, shall establish the process by
23 which the Secretary of Homeland Security
24 shares or releases information pursuant to
25 subparagraph (A).

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

4 (I) any sharing or release of in-
5 formation under subparagraph (A) is
6 made in accordance with voluntary
7 consensus standards for disclosure of
8 vulnerabilities; and

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

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

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

16 (I) the periodic review of
17 vulnerabilities that are determined by
18 the Board, pursuant to the process es-
19 tablished under paragraph (3)(A), not
20 to be shareable or releasable, in order
21 to determine whether such
22 vulnerabilities may be shared or re-
23 leased in a manner consistent with the
24 national security interests of the
25 United States; and

1 (II) the sharing with or releasing
2 to appropriate non-Federal entities of
3 information about vulnerabilities that
4 may be shared or released in a man-
5 ner consistent with the national secu-
6 rity interests of the United States fol-
7 lowing review under subclause (I).

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

10 (I) IN GENERAL.—In the case of
11 a vulnerability that was not publicly
12 known and determined not to be
13 shareable or releasable pursuant to
14 clause (i)(I) and then subsequently
15 becomes publicly known, the vulner-
16 ability shall not be subject to the
17 process established under paragraph
18 (3)(A) and shall be subject to such
19 other Federal procedures and inter-
20 agency operation processes as may be
21 applicable, such as procedures and
22 processes established to carry out the
23 Cybersecurity Information Sharing
24 Act of 2015 (6 U.S.C. 1501 et seq.).

1 (II) APPLICABILITY TO CLASSI-
2 FIED MATERIAL.—In this clause, sub-
3 paragraph (B) of subsection (a)(2)
4 shall not apply.

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

8 (f) OVERSIGHT.—

9 (1) ANNUAL REPORTS BY BOARD.—

10 (A) IN GENERAL.—Not less frequently
11 than once each year, the Board shall submit to
12 the appropriate committees of Congress a re-
13 port on the activities of the Board and the poli-
14 cies issued under subsection (d).

15 (B) CONTENTS.—In addition to informa-
16 tion about the activities and policies described
17 in subparagraph (A), the report required by
18 such subparagraph shall also include the fol-
19 lowing:

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

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

1 (iii) The number of vulnerabilities de-
2 termined by the Board to be shareable or
3 releasable.

4 (iv) The number of vulnerabilities de-
5 termined by the Board not to be shareable
6 or releasable.

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

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

13 (2) ANNUAL REPORTS ON ACTIVITIES OF IGS.—

14 (A) IN GENERAL.—Not less frequently
15 than once each year, the Inspector General of
16 the Department of Homeland Security shall, in
17 consultation with the Inspectors General of
18 other Federal agencies whose work is affected
19 by activities of the Board, submit to the appro-
20 priate committees of Congress a report on the
21 activities of all such Inspectors General during
22 the preceding year in connection with the activi-
23 ties of the Board, the policies issued under sub-
24 section (d), and the sharing and releasing of in-

1 formation about vulnerabilities pursuant to
2 such policies.

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

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

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

13 (A) IN GENERAL.—The Privacy and Civil
14 Liberties Oversight Board shall review each re-
15 port submitted under paragraph (1).

16 (B) CONSULTATION.—The Vulnerability
17 Equities Review Board may consult with the
18 Privacy and Civil Liberties Oversight Board as
19 the Vulnerability Equities Review Board con-
20 siders appropriate.

21 (5) APPROPRIATE COMMITTEES OF CONGRESS
22 DEFINED.—In this subsection, the term “appro-
23 priate committees of Congress” means—

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

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

4 (B) the Committee on Homeland Security,
5 the Committee on Oversight and Government
6 Reform, the Committee on Energy and Com-
7 merce, and the Permanent Select Committee on
8 Intelligence of the House of Representatives.