

HC-1

Pending

Chris Coons

AMENDMENT NO. \_\_\_\_\_

Calendar No. \_\_\_\_\_

Purpose: To modify section 5 to require DHS to review all cyber threat indicators and countermeasures in order to remove certain personal information.

IN THE SENATE OF THE UNITED STATES—114th Cong., 1st Sess.

S.754

Feinstein For By Coons	AMENDMENT N <sup>o</sup> 2552	through en- cybersecurity
To: Amdt. No. 2716		_____ and
754		inted
11		Coons
Page(s)		
GPO: 2014 91-623 (mac)		

- 1 Beginning on page <sup>23</sup>21, strike line <sup>3</sup>23 and all that fol-  
2 lows through page <sup>33</sup>31, line <sup>10</sup>5 and insert the following:
- 3 (3) REQUIREMENTS CONCERNING POLICIES AND  
4 PROCEDURES.—Consistent with the guidelines re-  
5 quired by subsection (b), the policies and procedures  
6 developed and promulgated under this subsection  
7 shall—
- 8 (A) ensure that cyber threat indicators  
9 shared with the Federal Government by any en-  
10 tity pursuant to section 4 that are received  
11 through the process described in subsection (c)

AS MODIFIED

1 of this section and that satisfy the requirements  
2 of the guidelines developed under subsection  
3 (b)—

4 (i) are shared in an automated man-  
5 ner with all of the appropriate Federal en-  
6 tities;

7 (ii) are not subject to any unnecessary  
8 delay, interference, or any other action  
9 that could impede receipt by all of the ap-  
10 propriate Federal entities; and

11 (iii) may be provided to other Federal  
12 entities;

13 (B) ensure that cyber threat indicators  
14 shared with the Federal Government by any en-  
15 tity pursuant to section 4 in a manner other  
16 than the process described in subsection (c) of  
17 this section—

18 (i) are shared as quickly as operation-  
19 ally practicable with all of the appropriate  
20 Federal entities;

21 (ii) are not subject to any unnecessary  
22 delay, interference, or any other action  
23 that could impede receipt by all of the ap-  
24 propriate Federal entities; and

1 (iii) may be provided to other Federal  
2 entities;

3 (C) consistent with this Act, any other ap-  
4 plicable provisions of law, and the fair informa-  
5 tion practice principles set forth in appendix A  
6 of the document entitled “National Strategy for  
7 Trusted Identities in Cyberspace” and pub-  
8 lished by the President in April 2011, govern  
9 the retention, use, and dissemination by the  
10 Federal Government of cyber threat indicators  
11 shared with the Federal Government under this  
12 Act, including the extent, if any, to which such  
13 cyber threat indicators may be used by the Fed-  
14 eral Government; and

15 (D) ensure there is—

16 (i) an audit capability; and

17 (ii) appropriate sanctions in place for  
18 officers, employees, or agents of a Federal  
19 entity who knowingly and willfully conduct  
20 activities under this Act in an unauthor-  
21 ized manner.

22 (4) GUIDELINES FOR ENTITIES SHARING CYBER  
23 THREAT INDICATORS WITH FEDERAL GOVERN-  
24 MENT.—

1           (A) IN GENERAL.—Not later than 60 days  
2 after the date of the enactment of this Act, the  
3 Attorney General shall develop and make pub-  
4 licly available guidance to assist entities and  
5 promote sharing of cyber threat indicators with  
6 Federal entities under this Act.

7           (B) CONTENTS.—The guidelines developed  
8 and made publicly available under subpara-  
9 graph (A) shall include guidance on the fol-  
10 lowing:

11           (i) Identification of types of informa-  
12 tion that would qualify as a cyber threat  
13 indicator under this Act that would be un-  
14 likely to include personal information of or  
15 identifying a specific person not necessary  
16 to describe or identify a cyber security  
17 threat.

18           (ii) Identification of types of informa-  
19 tion protected under otherwise applicable  
20 privacy laws that are unlikely to be nec-  
21 essary to describe or identify a cybersecu-  
22 rity threat.

23           (iii) Such other matters as the Attor-  
24 ney General considers appropriate for enti-

1                   ties sharing cyber threat indicators with  
2                   Federal entities under this Act.

3           (b) PRIVACY AND CIVIL LIBERTIES.—

4                   (1) GUIDELINES OF ATTORNEY GENERAL.—Not  
5           later than 60 days after the date of the enactment  
6           of this Act, the Attorney General shall, in coordina-  
7           tion with heads of the appropriate Federal entities  
8           and in consultation with officers designated under  
9           section 1062 of the National Security Intelligence  
10          Reform Act of 2004 (42 U.S.C. 2000ee-1), develop,  
11          submit to Congress, and make available to the public  
12          interim guidelines relating to privacy and civil lib-  
13          erties which shall govern the receipt, retention, use,  
14          and dissemination of cyber threat indicators by a  
15          Federal entity obtained in connection with activities  
16          authorized in this Act.

17                  (2) FINAL GUIDELINES.—

18                   (A) IN GENERAL.—Not later than 180  
19           days after the date of the enactment of this  
20           Act, the Attorney General shall, in coordination  
21           with heads of the appropriate Federal entities  
22           and in consultation with officers designated  
23           under section 1062 of the National Security In-  
24           telligence Reform Act of 2004 (42 U.S.C.  
25           2000ee-1) and such private entities with indus-

1 try expertise as the Attorney General considers  
2 relevant, promulgate final guidelines relating to  
3 privacy and civil liberties which shall govern the  
4 receipt, retention, use, and dissemination of  
5 cyber threat indicators by a Federal entity ob-  
6 tained in connection with activities authorized  
7 in this Act.

8 (B) PERIODIC REVIEW.—The Attorney  
9 General shall, in coordination with heads of the  
10 appropriate Federal entities and in consultation  
11 with officers and private entities described in  
12 subparagraph (A), periodically review the guide-  
13 lines promulgated under subparagraph (A).

14 (3) CONTENT.—The guidelines required by  
15 paragraphs (1) and (2) shall, consistent with the  
16 need to protect information systems from cybersecu-  
17 rity threats and mitigate cybersecurity threats—

18 (A) limit the impact on privacy and civil  
19 liberties of activities by the Federal Government  
20 under this Act;

21 (B) limit the receipt, retention, use, and  
22 dissemination of cyber threat indicators con-  
23 taining personal information of or identifying  
24 specific persons, including by establishing—

1 (i) a process for the timely destruction  
2 of such information that is known not to  
3 be directly related to uses authorized under  
4 this Act; and

5 (ii) specific limitations on the length  
6 of any period in which a cyber threat indi-  
7 cator may be retained;

8 (C) include requirements to safeguard  
9 cyber threat indicators containing personal in-  
10 formation of or identifying specific persons  
11 from unauthorized access or acquisition, includ-  
12 ing appropriate sanctions for activities by offi-  
13 cers, employees, or agents of the Federal Gov-  
14 ernment in contravention of such guidelines;

15 (D) include procedures for notifying enti-  
16 ties and Federal entities if information received  
17 pursuant to this section is known or determined  
18 by a Federal entity receiving such information  
19 not to constitute a cyber threat indicator;

20 (E) protect the confidentiality of cyber  
21 threat indicators containing personal informa-  
22 tion of or identifying specific persons to the  
23 greatest extent practicable and require recipi-  
24 ents to be informed that such indicators may

1           only be used for purposes authorized under this  
2           Act; and

3                   (F) include steps that may be needed so  
4           that dissemination of cyber threat indicators is  
5           consistent with the protection of classified and  
6           other sensitive national security information.

7           (c) CAPABILITY AND PROCESS WITHIN THE DEPART-  
8   MENT OF HOMELAND SECURITY.—

9                   (1) IN GENERAL.—Not later than 90 days after  
10          the date of the enactment of this Act, the Secretary  
11          of Homeland Security, in coordination with the  
12          heads of the appropriate Federal entities, shall de-  
13          velop and implement a capability and process within  
14          the Department of Homeland Security that—

15                   (A) shall accept from any entity in real  
16          time cyber threat indicators and defensive  
17          measures, pursuant to this section;

18                   (B) shall, upon submittal of the certifi-  
19          cation under paragraph (2) that such capability  
20          and process fully and effectively operates as de-  
21          scribed in such paragraph, be the process by  
22          which the Federal Government receives cyber  
23          threat indicators and defensive measures under  
24          this Act that are shared by a private entity with  
25          the Federal Government through electronic mail



1 or media, an interactive form on an Internet  
2 website, or a real time, automated process be-  
3 tween information systems except—

4 (i) communications between a Federal  
5 entity and a private entity regarding a pre-  
6 viously shared cyber threat indicator; and

7 (ii) communications by a regulated en-  
8 tity with such entity's Federal regulatory  
9 authority regarding a cybersecurity threat;

10 (C) shall require the Department of Home-  
11 land Security to review all cyber threat indica-  
12 tors and defensive measures received and re-  
13 move any personal information of or identifying  
14 a specific person not necessary to identify or  
15 describe the cybersecurity threat before sharing  
16 such indicator or defensive measure with appro-  
17 priate Federal entities;

18 (D) ensures that all of the appropriate  
19 Federal entities receive in an automated man-  
20 ner such cyber threat indicators as quickly as  
21 operationally possible from the Department of  
22 Homeland Security;

23 (E) is in compliance with the policies, pro-  
24 cedures, and guidelines required by this section;  
25 and

1 (F) does not limit or prohibit otherwise  
2 lawful disclosures of communications, records,  
3 or other information, including—

4 (i) reporting of known or suspected  
5 criminal activity, by an entity to any other  
6 entity or a Federal entity;

7 (ii) voluntary or legally compelled par-  
8 ticipation in a Federal investigation; and

9 (iii) providing cyber threat indicators  
10 or defensive measures as part of a statu-  
11 tory or authorized contractual requirement.

12 (2) CERTIFICATION.—Not later than 10 days  
13 prior to the implementation of the capability and  
14 process required by paragraph (1), the Secretary of  
15 Homeland Security shall, in consultation with the  
16 heads of the appropriate Federal entities, certify to  
17 Congress whether such capability and process fully  
18 and effectively operates—

19 (A) as the process by which the Federal  
20 Government receives from any entity a cyber  
21 threat indicator or defensive measure under this  
22 Act; and

23 (B) in accordance with the policies, proce-  
24 dures, and guidelines developed under this sec-  
25 tion.

1           (3) PUBLIC NOTICE AND ACCESS.—The Sec-  
2       retary of Homeland Security shall ensure there is  
3       public notice of, and access to, the capability and  
4       process developed and implemented under paragraph  
5       (1) so that—

6           (A) any entity may share cyber threat indi-  
7       cators and defensive measures through such  
8       process with the Federal Government; and

9           (B) all of the appropriate Federal entities  
10      receive such cyber threat indicators and defen-  
11      sive measures as quickly as operationally prac-  
12      ticable with receipt through the process within  
13      the Department of Homeland Security.