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

through en-
cybersecurity

_____ and

inted

Coons

AMENDMENT No. 2552

By Coons

To: S. 754

11

Page(s)

GPO: 2014 91-623 (mac)

Beginning on page 21, strike line 23 and all that follows through page 31, line 5 and insert the following:

(3) REQUIREMENTS CONCERNING POLICIES AND PROCEDURES.—Consistent with the guidelines required by subsection (b), the policies and procedures developed and promulgated under this subsection shall—

(A) ensure that cyber threat indicators shared with the Federal Government by any entity pursuant to section 4 that are received through the process described in subsection (c)

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

(i) are shared in an automated manner with all of the appropriate Federal entities;

(ii) are not subject to any unnecessary delay, interference, or any other action that could impede receipt by all of the appropriate Federal entities; and

(iii) may be provided to other Federal entities;

(B) ensure that cyber threat indicators shared with the Federal Government by any entity pursuant to section 4 in a manner other than the process described in subsection (c) of this section—

(i) are shared as quickly as operationally practicable with all of the appropriate Federal entities;

(ii) are not subject to any unnecessary delay, interference, or any other action that could impede receipt by all of the appropriate Federal entities; and

(iii) may be provided to other Federal entities;

(C) consistent with this Act, any other applicable provisions of law, and the fair information practice principles set forth in appendix A of the document entitled "National Strategy for Trusted Identities in Cyberspace" and published by the President in April 2011, govern the retention, use, and dissemination by the Federal Government of cyber threat indicators shared with the Federal Government under this Act, including the extent, if any, to which such cyber threat indicators may be used by the Federal Government; and

(D) ensure there is—

(i) an audit capability; and

(ii) appropriate sanctions in place for officers, employees, or agents of a Federal entity who knowingly and willfully conduct activities under this Act in an unauthorized manner.

(4) GUIDELINES FOR ENTITIES SHARING CYBER THREAT INDICATORS WITH FEDERAL GOVERNMENT.—

(A) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Attorney General shall develop and make publicly available guidance to assist entities and promote sharing of cyber threat indicators with Federal entities under this Act.

(B) CONTENTS.—The guidelines developed and made publicly available under subparagraph (A) shall include guidance on the following:

(i) Identification of types of information that would qualify as a cyber threat indicator under this Act that would be unlikely to include personal information of or identifying a specific person not necessary to describe or identify a cyber security threat.

(ii) Identification of types of information protected under otherwise applicable privacy laws that are unlikely to be necessary to describe or identify a cybersecurity threat.

(iii) Such other matters as the Attorney General considers appropriate for enti-

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

(b) PRIVACY AND CIVIL LIBERTIES.—

(1) GUIDELINES OF ATTORNEY GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers designated under section 1062 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee–1), develop, submit to Congress, and make available to the public interim guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this Act.

(2) FINAL GUIDELINES.—

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

try expertise as the Attorney General considers relevant, promulgate final guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this Act.

(B) PERIODIC REVIEW.—The Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers and private entities described in subparagraph (A), periodically review the guidelines promulgated under subparagraph (A).

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

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

(B) limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information of or identifying specific persons, including by establishing—

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

(ii) specific limitations on the length of any period in which a cyber threat indicator may be retained;

(C) include requirements to safeguard cyber threat indicators containing personal information of or identifying specific persons from unauthorized access or acquisition, including appropriate sanctions for activities by officers, employees, or agents of the Federal Government in contravention of such guidelines;

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

(E) protect the confidentiality of cyber threat indicators containing personal information of or identifying specific persons to the greatest extent practicable and require recipients to be informed that such indicators may

only be used for purposes authorized under this Act; and

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

(c) CAPABILITY AND PROCESS WITHIN THE DEPARTMENT OF HOMELAND SECURITY.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security, in coordination with the heads of the appropriate Federal entities, shall develop and implement a capability and process within the Department of Homeland Security that—

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

(B) shall, upon submittal of the certification under paragraph (2) that such capability and process fully and effectively operates as described in such paragraph, be the process by which the Federal Government receives cyber threat indicators and defensive measures under this Act that are shared by a private entity with the Federal Government through electronic mail

or media, an interactive form on an Internet website, or a real time, automated process between information systems except—

(i) communications between a Federal entity and a private entity regarding a previously shared cyber threat indicator; and

(ii) communications by a regulated entity with such entity's Federal regulatory authority regarding a cybersecurity threat;

(C) shall require the Department of Homeland Security to review all cyber threat indicators and defensive measures received and remove any personal information of or identifying a specific person not necessary to identify or describe the cybersecurity threat before sharing such indicator or defensive measure with appropriate Federal entities;

(D) ensures that all of the appropriate Federal entities receive in an automated manner such cyber threat indicators as quickly as operationally possible from the Department of Homeland Security;

(E) is in compliance with the policies, procedures, and guidelines required by this section; and

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

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

(ii) voluntary or legally compelled participation in a Federal investigation; and

(iii) providing cyber threat indicators or defensive measures as part of a statutory or authorized contractual requirement.

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

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

(B) in accordance with the policies, procedures, and guidelines developed under this section.

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

(A) any entity may share cyber threat indicators and defensive measures through such process with the Federal Government; and

(B) all of the appropriate Federal entities receive such cyber threat indicators and defensive measures as quickly as operationally practicable with receipt through the process within the Department of Homeland Security.