Union Calendar No. 61

114TH CONGRESS
1ST SESSION

H. R. 1731

[Report No. 114–83]

To amend the Homeland Security Act of 2002 to enhance multi-directional sharing of information related to cybersecurity risks and strengthen privacy and civil liberties protections, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

APRIL 13, 2015

Mr. MCCAUL (for himself and Mr. RATCLIFFE) introduced the following bill; which was referred to the Committee on Homeland Security

APRIL 17, 2015

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed

[Strike out all after the enacting clause and insert the part printed in italic]

[For text of introduced bill, see copy of bill as introduced on April 13, 2015]

A BILL

To amend the Homeland Security Act of 2002 to enhance multi-directional sharing of information related to cybersecurity risks and strengthen privacy and civil liberties protections, 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 "National Cybersecurity Protection Advancement Act of 2015".

SEC. 2. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

(a) DEFINITIONS.—

(1) IN GENERAL.—Subsection (a) of the second section 226 of the Homeland Security Act of 2002 (6 U.S.C. 148; relating to the National Cybersecurity and Communications Integration Center) is amended—

(A) in paragraph (3), by striking "and" at the end;

(B) in paragraph (4), by striking the period at the end and inserting "; and"; and

(C) by adding at the end the following new paragraphs:

"(5) the term 'cyber threat indicator' means technical information that is necessary to describe or identify—

"(A) a method for probing, monitoring, maintaining, or establishing network awareness of an information system for the purpose of dis-

cerning technical vulnerabilities of such information system, if such method is known or reasonably suspected of being associated with a known or suspected cybersecurity risk, including communications that reasonably appear to be transmitted for the purpose of gathering technical information related to a cybersecurity risk;

"(B) a method for defeating a technical or security control of an information system;

"(C) a technical vulnerability, including anomalous technical behavior that may become a vulnerability;

"(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to inadvertently enable the defeat of a technical or operational control;

"(E) a method for unauthorized remote identification of, access to, or use of an information system or information that is stored on, processed by, or transiting an information system that is known or reasonably suspected of being associated with a known or suspected cybersecurity risk;

"(F) the actual or potential harm caused by a cybersecurity risk, including a description of the information exfiltrated as a result of a particular cybersecurity risk;

"(G) any other attribute of a cybersecurity risk that cannot be used to identify specific persons reasonably believed to be unrelated to such cybersecurity risk, if disclosure of such attribute is not otherwise prohibited by law; or

"(H) any combination of subparagraphs (A) through (G);

"(6) the term 'cybersecurity purpose' means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity risk or incident;

"(7)(A) except as provided in subparagraph (B), the term 'defensive measure' means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity risk or incident, or any attribute of hardware, software, process, or procedure

that could enable or facilitate the defeat of a security control;

"(B) such term does not include a measure that destroys, renders unusable, or substantially harms an information system or data on an information system not belonging to—

"(i) the non-Federal entity, not including a State, local, or tribal government, operating such measure; or

"(ii) another Federal entity or non-Federal entity that is authorized to provide consent and has provided such consent to the non-Federal entity referred to in clause (i);

"(8) the term 'network awareness' means to scan, identify, acquire, monitor, log, or analyze information that is stored on, processed by, or transiting an information system;

"(9)(A) the term 'private entity' means a non-Federal entity that is an individual or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or non-profit entity, including an officer, employee, or agent thereof;

"(B) such term includes a component of a State, local, or tribal government performing electric utility services;

"(10) the term 'security control' means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentially, integrity, or availability of an information system or information that is stored on, processed by, or transiting an information system; and

"(11) the term 'sharing' means providing, receiving, and disseminating.".

(b) AMENDMENT.—Subparagraph (B) of subsection (d)(1) of such second section 226 of the Homeland Security Act of 2002 is amended—

(1) in clause (i), by striking "and local" and inserting ", local, and tribal";

(2) in clause (ii)—

(A) by inserting ", including information sharing and analysis centers" before the semicolon; and

(B) by striking "and" at the end;

(3) in clause (iii), by striking the period at the end and inserting "; and"; and

(4) by adding at the end the following new clause:

"(iv) private entities.".

SEC. 3. INFORMATION SHARING STRUCTURE AND PROCESSES.

The second section 226 of the Homeland Security Act of 2002 (6 U.S.C. 148; relating to the National Cybersecurity and Communications Integration Center) is amended—

(1) in subsection (c)—

(A) in paragraph (1)—

(i) by striking "a Federal civilian interface" and inserting "the lead Federal civilian interface"; and

(ii) by striking "cybersecurity risks," and inserting "cyber threat indicators, defensive measures, cybersecurity risks,";

(B) in paragraph (3), by striking "cybersecurity risks" and inserting "cyber threat indicators, defensive measures, cybersecurity risks,";

(C) in paragraph (5)(A), by striking "cybersecurity risks" and inserting "cyber threat indicators, defensive measures, cybersecurity risks,";

(D) in paragraph (6)—

(i) by striking "cybersecurity risks" and inserting "cyber threat indicators, defensive measures, cybersecurity risks,"; and

(ii) by striking "and" at the end;

(E) in paragraph (7)—

(i) in subparagraph (A), by striking "and" at the end;

(ii) in subparagraph (B), by striking the period at the end and inserting "; and"; and

(iii) by adding at the end the following new subparagraph:

"(C) sharing cyber threat indicators and defensive measures;"; and

(F) by adding at the end the following new paragraphs

"(8) engaging with international partners, in consultation with other appropriate agencies, to—

"(A) collaborate on cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents; and

"(B) enhance the security and resilience of global cybersecurity;

"(9) sharing cyber threat indicators, defensive measures, and other information related to cybersecu-

rity risks and incidents with Federal and non-Federal entities, including across sectors of critical infrastructure and with State and major urban area fusion centers, as appropriate;

"(10) promptly notifying the Secretary and the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate of any significant violations of the policies and procedures specified in subsection (i)(6)(A);

"(11) promptly notifying non-Federal entities that have shared cyber threat indicators or defensive measures that are known or determined to be in error or in contravention of the requirements of this section; and

"(12) participating, as appropriate, in exercises run by the Department's National Exercise Program.";

(2) in subsection (d)—

(A) in subparagraph (D), by striking "and" at the end;

(B) by redesignating subparagraph (E) as subparagraph (J); and

(C) by inserting after subparagraph (D) the following new subparagraphs:

"(E) an entity that collaborates with State and local governments on cybersecurity risks and incidents, and has entered into a voluntary information sharing relationship with the Center;

"(F) a United States Computer Emergency Readiness Team that coordinates information related to cybersecurity risks and incidents, proactively and collaboratively addresses cybersecurity risks and incidents to the United States, collaboratively responds to cybersecurity risks and incidents, provides technical assistance, upon request, to information system owners and operators, and shares cyber threat indicators, defensive measures, analysis, or information related to cybersecurity risks and incidents in a timely manner;

"(G) the Industrial Control System Cyber Emergency Response Team that—

"(i) coordinates with industrial control systems owners and operators;

"(ii) provides training, upon request, to Federal entities and non-Federal entities on industrial control systems cybersecurity;

"(iii) collaboratively addresses cybersecurity risks and incidents to industrial control systems;

"(iv) provides technical assistance, upon request, to Federal entities and non-Federal entities relating to industrial control systems cybersecurity; and

"(v) shares cyber threat indicators, defensive measures, or information related to cybersecurity risks and incidents of industrial control systems in a timely fashion;

"(H) a National Coordinating Center for Communications that coordinates the protection, response, and recovery of emergency communications;

"(I) an entity that coordinates with small and medium-sized businesses; and";

(3) in subsection (e)—

(A) in paragraph (1)—

(i) in subparagraph (A), by inserting "cyber threat indicators, defensive measures, and" before "information";

(ii) in subparagraph (B), by inserting "cyber threat indicators, defensive measures, and" before "information";

(iii) in subparagraph (F), by striking "cybersecurity risks" and inserting "cyber threat indicators, defensive measures, cybersecurity risks,";

(iv) in subparagraph (F), by striking "and" at the end;

(v) in subparagraph (G), by striking "cybersecurity risks" and inserting "cyber threat indicators, defensive measures, cybersecurity risks,"; and

(vi) by adding at the end the following:

"(H) the Center ensures that it shares information relating to cybersecurity risks and incidents with small and medium-sized businesses, as appropriate; and

"(I) the Center designates an agency contact for non-Federal entities;";

(B) in paragraph (2)—

(i) by striking "cybersecurity risks" and inserting "cyber threat indicators, defensive measures, cybersecurity risks,"; and

(ii) by inserting "or disclosure" before the semicolon at the end; and

(C) in paragraph (3), by inserting before the period at the end the following: ", including

by working with the Chief Privacy Officer appointed under section 222 to ensure that the Center follows the policies and procedures specified in subsection (i)(6)(A)"; and

(4) by adding at the end the following new subsections:

"(g) RAPID AUTOMATED SHARING.—

"(1) IN GENERAL.—The Under Secretary for Cybersecurity and Infrastructure Protection, in coordination with industry and other stakeholders, shall develop capabilities making use of existing information technology industry standards and best practices, as appropriate, that support and rapidly advance the development, adoption, and implementation of automated mechanisms for the timely sharing of cyber threat indicators and defensive measures to and from the Center and with each Federal agency designated as the 'Sector Specific Agency' for each critical infrastructure sector in accordance with subsection (h).

"(2) BIANNUAL REPORT.—The Under Secretary for Cybersecurity and Infrastructure Protection shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a biannual report on the status and progress

of the development of the capability described in paragraph (1). Such reports shall be required until such capability is fully implemented.

"(h) SECTOR SPECIFIC AGENCIES.—The Secretary, in collaboration with the relevant critical infrastructure sector and the heads of other appropriate Federal agencies, shall recognize the Federal agency designated as of March 25, 2015, as the 'Sector Specific Agency' for each critical infrastructure sector designated in the Department's National Infrastructure Protection Plan. If the designated Sector Specific Agency for a particular critical infrastructure sector is the Department, for purposes of this section, the Secretary is deemed to be the head of such Sector Specific Agency and shall carry out this section. The Secretary, in coordination with the heads of each such Sector Specific Agency, shall—

"(1) support the security and resilience actives of the relevant critical infrastructure sector in accordance with this section;

"(2) provide institutional knowledge, specialized expertise, and technical assistance upon request to the relevant critical infrastructure sector; and

"(3) support the timely sharing of cyber threat indicators and defensive measures with the relevant

critical infrastructure sector with the Center in accordance with this section.

"(i) VOLUNTARY INFORMATION SHARING PROCEDURES.—

"(1) PROCEDURES.—

"(A) IN GENERAL.—The Center may enter into a voluntary information sharing relationship with any consenting non-Federal entity for the sharing of cyber threat indicators and defensive measures for cybersecurity purposes in accordance with this section. Nothing in this section may be construed to require any non-Federal entity to enter into any such information sharing relationship with the Center or any other entity. The Center may terminate a voluntary information sharing relationship under this subsection if the Center determines that the non-Federal entity with which the Center has entered into such a relationship has, after repeated notice, repeatedly violated the terms of this subsection.

"(B) NATIONAL SECURITY.—The Secretary may decline to enter into a voluntary information sharing relationship under this subsection if

the Secretary determines that such is appropriate for national security.

"(2) VOLUNTARY INFORMATION SHARING RELATIONSHIPS.—A voluntary information sharing relationship under this subsection may be characterized as an agreement described in this paragraph.

"(A) STANDARD AGREEMENT.—For the use of a non-Federal entity, the Center shall make available a standard agreement, consistent with this section, on the Department's website.

"(B) NEGOTIATED AGREEMENT.—At the request of a non-Federal entity, and if determined appropriate by the Center, the Department shall negotiate a non-standard agreement, consistent with this section.

"(C) EXISTING AGREEMENTS.—An agreement between the Center and a non-Federal entity that is entered into before the date of the enactment of this section, or such an agreement that is in effect before such date, shall be deemed in compliance with the requirements of this subsection, notwithstanding any other provision or requirement of this subsection. An agreement under this subsection shall include the relevant privacy protections as in effect under the Cooper-

ative Research and Development Agreement for Cybersecurity Information Sharing and Collaboration, as of December 31, 2014. Nothing in this subsection may be construed to require a non-Federal entity to enter into either a standard or negotiated agreement to be in compliance with this subsection.

"(3) INFORMATION SHARING AUTHORIZATION.—

"(A) IN GENERAL.—Except as provided in subparagraph (B), and notwithstanding any other provision of law, a non-Federal entity may, for cybersecurity purposes, share cyber threat indicators or defensive measures obtained on its own information system, or on an information system of another Federal entity or non-Federal entity, upon written consent of such other Federal entity or non-Federal entity or an authorized representative of such other Federal entity or non-Federal entity in accordance with this section with—

"(i) another non-Federal entity; or

"(ii) the Center, as provided in this section.

"(B) LAWFUL RESTRICTION.—A non-Federal entity receiving a cyber threat indicator or

defensive measure from another Federal entity or non-Federal entity shall comply with otherwise lawful restrictions placed on the sharing or use of such cyber threat indicator or defensive measure by the sharing Federal entity or non-Federal entity.

"(C) REMOVAL OF INFORMATION UNRELATED TO CYBERSECURITY RISKS OR INCIDENTS.—Federal entities and non-Federal entities shall, prior to such sharing, take reasonable efforts to remove information that can be used to identify specific persons and is reasonably believed at the time of sharing to be unrelated to a cybersecurity risks or incident and to safeguard information that can be used to identify specific persons from unintended disclosure or unauthorized access or acquisition.

"(D) RULE OF CONSTRUCTION.—Nothing in this paragraph may be construed to—

"(i) limit or modify an existing information sharing relationship;

"(ii) prohibit a new information sharing relationship;

"(iii) require a new information sharing relationship between any non-Federal entity and a Federal entity;

"(iv) limit otherwise lawful activity; or

"(v) in any manner impact or modify procedures in existence as of the date of the enactment of this section for reporting known or suspected criminal activity to appropriate law enforcement authorities or for participating voluntarily or under legal requirement in an investigation.

"(E) COORDINATED VULNERABILITY DISCLOSURE.—The Under Secretary for Cybersecurity and Infrastructure Protection, in coordination with industry and other stakeholders, shall develop, publish, and adhere to policies and procedures for coordinating vulnerability disclosures, to the extent practicable, consistent with international standards in the information technology industry.

"(4) NETWORK AWARENESS AUTHORIZATION.—

"(A) IN GENERAL.—Notwithstanding any other provision of law, a non-Federal entity, not including a State, local, or tribal government,

may, for cybersecurity purposes, conduct network awareness of—

"(i) an information system of such non-Federal entity to protect the rights or property of such non-Federal entity;

"(ii) an information system of another non-Federal entity, upon written consent of such other non-Federal entity for conducting such network awareness to protect the rights or property of such other non-Federal entity;

"(iii) an information system of a Federal entity, upon written consent of an authorized representative of such Federal entity for conducting such network awareness to protect the rights or property of such Federal entity; or

"(iv) information that is stored on, processed by, or transiting an information system described in this subparagraph.

"(B) RULE OF CONSTRUCTION.—Nothing in this paragraph may be construed to—

"(i) authorize conducting network awareness of an information system, or the use of any information obtained through

such conducting of network awareness, other than as provided in this section; or

"(ii) limit otherwise lawful activity.

"(5) DEFENSIVE MEASURE AUTHORIZATION.—

"(A) IN GENERAL.—Except as provided in subparagraph (B) and notwithstanding any other provision of law, a non-Federal entity, not including a State, local, or tribal government, may, for cybersecurity purposes, operate a defensive measure that is applied to—

"(i) an information system of such non-Federal entity to protect the rights or property of such non-Federal entity;

"(ii) an information system of another non-Federal entity upon written consent of such other non-Federal entity for operation of such defensive measure to protect the rights or property of such other non-Federal entity;

"(iii) an information system of a Federal entity upon written consent of an authorized representative of such Federal entity for operation of such defensive measure to protect the rights or property of such Federal entity; or

"(iv) information that is stored on, processed by, or transiting an information system described in this subparagraph.

"(B) RULE OF CONSTRUCTION.—Nothing in this paragraph may be construed to—

"(i) authorize the use of a defensive measure other than as provided in this section; or

"(ii) limit otherwise lawful activity.

"(6) PRIVACY AND CIVIL LIBERTIES PROTECTIONS.—

"(A) POLICIES AND PROCEDURES.—

"(i) IN GENERAL.—The Under Secretary for Cybersecurity and Infrastructure Protection shall, in coordination with the Chief Privacy Officer and the Chief Civil Rights and Civil Liberties Officer of the Department, establish and annually review policies and procedures governing the receipt, retention, use, and disclosure of cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents shared with the Center in accordance with this section. Such policies and procedures shall apply only to the De-

partment, consistent with the need to protect information systems from cybersecurity risks and incidents and mitigate cybersecurity risks and incidents in a timely manner, and shall—

"(I) be consistent with the Department's Fair Information Practice Principles developed pursuant to section 552a of title 5, United States Code (commonly referred to as the 'Privacy Act of 1974' or the 'Privacy Act'), and subject to the Secretary's authority under subsection (a)(2) of section 222 of this Act;

"(II) reasonably limit, to the greatest extent practicable, the receipt, retention, use, and disclosure of cyber threat indicators and defensive measures associated with specific persons that is not necessary, for cybersecurity purposes, to protect a network or information system from cybersecurity risks or mitigate cybersecurity risks and incidents in a timely manner;

"(III) minimize any impact on privacy and civil liberties;

"(IV) provide data integrity through the prompt removal and destruction of obsolete or erroneous names and personal information that is unrelated to the cybersecurity risk or incident information shared and retained by the Center in accordance with this section;

"(V) include requirements to safeguard cyber threat indicators and defensive measures retained by the Center, including information that is proprietary or business-sensitive that may be used to identify specific persons from unauthorized access or acquisition;

"(VI) protect the confidentiality of cyber threat indicators and defensive measures associated with specific persons to the greatest extent practicable; and

"(VII) ensure all relevant constitutional, legal, and privacy protections are observed.

"(ii) SUBMISSION TO CONGRESS.—Not later than 180 days after the date of the enactment of this section and annually thereafter, the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department, in consultation with the Privacy and Civil Liberties Oversight Board (established pursuant to section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee)), shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate the policies and procedures governing the sharing of cyber threat indicators, defensive measures, and information related to cybsersecurity risks and incidents described in clause (i) of subparagraph (A).

"(iii) PUBLIC NOTICE AND ACCESS.—The Under Secretary for Cybersecurity and Infrastructure Protection, in consultation

with the Chief Privacy Officer and the Chief Civil Rights and Civil Liberties Officer of the Department, and the Privacy and Civil Liberties Oversight Board (established pursuant to section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee)), shall ensure there is public notice of, and access to, the policies and procedures governing the sharing of cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents.

"(iv) CONSULTATION.—The Under Secretary for Cybersecurity and Infrastructure Protection when establishing policies and procedures to support privacy and civil liberties may consult with the National Institute of Standards and Technology.

"(B) IMPLEMENTATION.—The Chief Privacy Officer of the Department, on an ongoing basis, shall—

"(i) monitor the implementation of the policies and procedures governing the sharing of cyber threat indicators and defensive

measures established pursuant to clause (i) of subparagraph (A);

"(ii) regularly review and update privacy impact assessments, as appropriate, to ensure all relevant constitutional, legal, and privacy protections are being followed;

"(iii) work with the Under Secretary for Cybersecurity and Infrastructure Protection to carry out paragraphs (10) and (11) of subsection (c);

"(iv) annually submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that contains a review of the effectiveness of such policies and procedures to protect privacy and civil liberties; and

"(v) ensure there are appropriate sanctions in place for officers, employees, or agents of the Department who intentionally or willfully conduct activities under this section in an unauthorized manner.

"(C) INSPECTOR GENERAL REPORT.—The Inspector General of the Department, in con-

sultation with the Privacy and Civil Liberties Oversight Board and the Inspector General of each Federal agency that receives cyber threat indicators or defensive measures shared with the Center under this section, shall, not later than two years after the date of the enactment of this subsection and periodically thereafter submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report containing a review of the use of cybersecurity risk information shared with the Center, including the following:

"(i) A report on the receipt, use, and dissemination of cyber threat indicators and defensive measures that have been shared with Federal entities under this section.

"(ii) Information on the use by the Center of such information for a purpose other than a cybersecurity purpose.

"(iii) A review of the type of information shared with the Center under this section.

"(iv) A review of the actions taken by the Center based on such information.

"(v) The appropriate metrics that exist to determine the impact, if any, on privacy and civil liberties as a result of the sharing of such information with the Center.

"(vi) A list of other Federal agencies receiving such information.

"(vii) A review of the sharing of such information within the Federal Government to identify inappropriate stove piping of such information.

"(viii) Any recommendations of the Inspector General of the Department for improvements or modifications to information sharing under this section.

"(D) PRIVACY AND CIVIL LIBERTIES OFFICERS REPORT.—The Chief Privacy Officer and the Chief Civil Rights and Civil Liberties Officer of the Department, in consultation with the Privacy and Civil Liberties Oversight Board, the Inspector General of the Department, and the senior privacy and civil liberties officer of each Federal agency that receives cyber threat indicators and defensive measures shared with the Center under this section, shall biennially submit to the appropriate congressional committees a re-

port assessing the privacy and civil liberties impact of the activities under this paragraph. Each such report shall include any recommendations the Chief Privacy Officer and the Chief Civil Rights and Civil Liberties Officer of the Department consider appropriate to minimize or mitigate the privacy and civil liberties impact of the sharing of cyber threat indicators and defensive measures under this section.

"(E) FORM.—Each report required under paragraphs (C) and (D) shall be submitted in unclassified form, but may include a classified annex.

"(7) USES AND PROTECTION OF INFORMATION.—

"(A) NON-FEDERAL ENTITIES.—A non-Federal entity, not including a State, local, or tribal government, that shares cyber threat indicators or defensive measures through the Center or otherwise under this section—

"(i) may use, retain, or further disclose such cyber threat indicators or defensive measures solely for cybersecurity purposes;

"(ii) shall, prior to such sharing, take reasonable efforts to remove information that can be used to identify specific persons

and is reasonably believed at the time of sharing to be unrelated to a cybersecurity risk or incident, and to safeguard information that can be used to identify specific persons from unintended disclosure or unauthorized access or acquisition;

"(iii) shall comply with appropriate restrictions that a Federal entity or non-Federal entity places on the subsequent disclosure or retention of cyber threat indicators and defensive measures that it discloses to other Federal entities or non-Federal entities;

"(iv) shall be deemed to have voluntarily shared such cyber threat indicators or defensive measures;

"(v) shall implement and utilize a security control to protect against unauthorized access to or acquisition of such cyber threat indicators or defensive measures; and

"(vi) may not use such information to gain an unfair competitive advantage to the detriment of any non-Federal entity.

"(B) FEDERAL ENTITIES.—

"(i) USES OF INFORMATION.—A Federal entity that receives cyber threat indicators or defensive measures shared through the Center or otherwise under this section from another Federal entity or a non-Federal entity—

"(I) may use, retain, or further disclose such cyber threat indicators or defensive measures solely for cybersecurity purposes;

"(II) shall, prior to such sharing, take reasonable efforts to remove information that can be used to identify specific persons and is reasonably believed at the time of sharing to be unrelated to a cybersecurity risk or incident, and to safeguard information that can be used to identify specific persons from unintended disclosure or unauthorized access or acquisition;

"(III) shall be deemed to have voluntarily shared such cyber threat indicators or defensive measures;

"(IV) shall implement and utilize a security control to protect against

unauthorized access to or acquisition of such cyber threat indicators or defensive measures; and

"(V) may not use such cyber threat indicators or defensive measures to engage in surveillance or other collection activities for the purpose of tracking an individual's personally identifiable information.

"(ii) PROTECTIONS FOR INFORMATION.—The cyber threat indicators and defensive measures referred to in clause (i)—

"(I) are exempt from disclosure under section 552 of title 5, United States Code, and withheld, without discretion, from the public under subsection (b)(3)(B) of such section;

"(II) may not be used by the Federal Government for regulatory purposes;

"(III) may not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection;

"(IV) shall be considered the commercial, financial, and proprietary information of the non-Federal entity referred to in clause (i) when so designated by such non-Federal entity; and

"(V) may not be subject to a rule of any Federal entity or any judicial doctrine regarding ex parte communications with a decisionmaking official.

"(C) STATE, LOCAL, OR TRIBAL GOVERNMENT.—

"(i) USES OF INFORMATION.—A State, local, or tribal government that receives cyber threat indicators or defensive measures from the Center from a Federal entity or a non-Federal entity—

"(I) may use, retain, or further disclose such cyber threat indicators or defensive measures solely for cybersecurity purposes;

"(II) shall, prior to such sharing, take reasonable efforts to remove information that can be used to identify

specific persons and is reasonably believed at the time of sharing to be unrelated to a cybersecurity risk or incident, and to safeguard information that can be used to identify specific persons from unintended disclosure or unauthorized access or acquisition;

"(III) shall consider such information the commercial, financial, and proprietary information of such Federal entity or non-Federal entity if so designated by such Federal entity or non-Federal entity;

"(IV) shall be deemed to have voluntarily shared such cyber threat indicators or defensive measures; and

"(V) shall implement and utilize a security control to protect against unauthorized access to or acquisition of such cyber threat indicators or defensive measures.

"(ii) PROTECTIONS FOR INFORMATION.—The cyber threat indicators and defensive measures referred to in clause (i)—

"(I) shall be exempt from disclosure under any State, local, or tribal law or regulation that requires public disclosure of information or records by a public or quasi-public entity; and

"(II) may not be used by any State, local, or tribal government to regulate a lawful activity of a non-Federal entity.

"(8) LIABILITY EXEMPTIONS.—

"(A) NETWORK AWARENESS.—No cause of action shall lie or be maintained in any court, and such action shall be promptly dismissed, against any non-Federal entity that, for cybersecurity purposes, conducts network awareness under paragraph (4), if such network awareness is conducted in accordance with such paragraph and this section.

"(B) INFORMATION SHARING.—No cause of action shall lie or be maintained in any court, and such action shall be promptly dismissed, against any non-Federal entity that, for cybersecurity purposes, shares cyber threat indicators or defensive measures under paragraph (3), or fails to act based on such sharing, if such sharing is

conducted in accordance with such paragraph and this section.

"(C) WILLFUL MISCONDUCT.—

"(i) RULE OF CONSTRUCTION.—Nothing in this section may be construed to—

"(I) require dismissal of a cause of action against a non-Federal entity that has engaged in willful misconduct in the course of conducting activities authorized by this section; or

"(II) undermine or limit the availability of otherwise applicable common law or statutory defenses.

"(ii) PROOF OF WILLFUL MISCONDUCT.—In any action claiming that subparagraph (A) or (B) does not apply due to willful misconduct described in clause (i), the plaintiff shall have the burden of proving by clear and convincing evidence the willful misconduct by each non-Federal entity subject to such claim and that such willful misconduct proximately caused injury to the plaintiff.

"(iii) WILLFUL MISCONDUCT DEFINED.—In this subsection, the term 'willful

misconduct' means an act or omission that is taken—

"(I) intentionally to achieve a wrongful purpose;

"(II) knowingly without legal or factual justification; and

"(III) in disregard of a known or obvious risk that is so great as to make it highly probable that the harm will outweigh the benefit.

"(D) EXCLUSION.—The term 'non-Federal entity' as used in this paragraph shall not include a State, local, or tribal government.

"(9) FEDERAL GOVERNMENT LIABILITY FOR VIOLATIONS OF RESTRICTIONS ON THE USE AND PROTECTION OF VOLUNTARILY SHARED INFORMATION.—

"(A) IN GENERAL.—If a department or agency of the Federal Government intentionally or willfully violates the restrictions specified in paragraph (3), (6), or (7)(B) on the use and protection of voluntarily shared cyber threat indicators or defensive measures, or any other provision of this section, the Federal Government shall be liable to a person injured by such violation in an amount equal to the sum of—

"(i) the actual damages sustained by such person as a result of such violation or $1,000, whichever is greater; and

"(ii) reasonable attorney fees as determined by the court and other litigation costs reasonably occurred in any case under this subsection in which the complainant has substantially prevailed.

"(B) VENUE.—An action to enforce liability under this subsection may be brought in the district court of the United States in—

"(i) the district in which the complainant resides;

"(ii) the district in which the principal place of business of the complainant is located;

"(iii) the district in which the department or agency of the Federal Government that disclosed the information is located; or

"(iv) the District of Columbia.

"(C) STATUTE OF LIMITATIONS.—No action shall lie under this subsection unless such action is commenced not later than two years after the date of the violation of any restriction specified in paragraph (3), (6), or 7(B), or any other pro-

vision of this section, that is the basis for such action.

"(D) EXCLUSIVE CAUSE OF ACTION.—A cause of action under this subsection shall be the exclusive means available to a complainant seeking a remedy for a violation of any restriction specified in paragraph (3), (6), or 7(B) or any other provision of this section.

"(10) ANTI-TRUST EXEMPTION.—

"(A) IN GENERAL.—Except as provided in subparagraph (C), it shall not be considered a violation of any provision of antitrust laws for two or more non-Federal entities to share a cyber threat indicator or defensive measure, or assistance relating to the prevention, investigation, or mitigation of a cybersecurity risk or incident, for cybersecurity purposes under this Act.

"(B) APPLICABILITY.—Subparagraph (A) shall apply only to information that is shared or assistance that is provided in order to assist with—

"(i) facilitating the prevention, investigation, or mitigation of a cybersecurity risk or incident to an information system

or information that is stored on, processed by, or transiting an information system; or

"(ii) communicating or disclosing a cyber threat indicator or defensive measure to help prevent, investigate, or mitigate the effect of a cybersecurity risk or incident to an information system or information that is stored on, processed by, or transiting an information system.

"(C) PROHIBITED CONDUCT.—Nothing in this section may be construed to permit price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, or exchanges of price or cost information, customer lists, or information regarding future competitive planning.

"(11) CONSTRUCTION AND PREEMPTION.—

"(A) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this section may be construed to limit or prohibit otherwise lawful disclosures of communications, records, or other information, including reporting of known or suspected criminal activity or participating voluntarily or under legal requirement in an investigation, by a non-

Federal to any other non-Federal entity or Federal entity under this section.

"(B) WHISTLE BLOWER PROTECTIONS.—Nothing in this section may be construed to prohibit or limit the disclosure of information protected under section 2302(b)(8) of title 5, United States Code (governing disclosures of illegality, waste, fraud, abuse, or public health or safety threats), section 7211 of title 5, United States Code (governing disclosures to Congress), section 1034 of title 10, United States Code (governing disclosure to Congress by members of the military), section 1104 of the National Security Act of 1947 (50 U.S.C. 3234) (governing disclosure by employees of elements of the intelligence community), or any similar provision of Federal or State law.

"(C) RELATIONSHIP TO OTHER LAWS.—Nothing in this section may be construed to affect any requirement under any other provision of law for a non-Federal entity to provide information to a Federal entity.

"(D) PRESERVATION OF CONTRACTUAL OBLIGATIONS AND RIGHTS.—Nothing in this section may be construed to—

"(i) amend, repeal, or supersede any current or future contractual agreement, terms of service agreement, or other contractual relationship between any non-Federal entities, or between any non-Federal entity and a Federal entity; or

"(ii) abrogate trade secret or intellectual property rights of any non-Federal entity or Federal entity.

"(E) ANTI-TASKING RESTRICTION.—Nothing in this section may be construed to permit a Federal entity to—

"(i) require a non-Federal entity to provide information to a Federal entity;

"(ii) condition the sharing of cyber threat indicators or defensive measures with a non-Federal entity on such non-Federal entity's provision of cyber threat indicators or defensive measures to a Federal entity; or

"(iii) condition the award of any Federal grant, contract, or purchase on the sharing of cyber threat indicators or defensive measures with a Federal entity.

"(F) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this section may be construed

to subject any non-Federal entity to liability for choosing to not engage in the voluntary activities authorized under this section.

"(G) USE AND RETENTION OF INFORMATION.—Nothing in this section may be construed to authorize, or to modify any existing authority of, a department or agency of the Federal Government to retain or use any information shared under this section for any use other than permitted in this section.

"(H) VOLUNTARY SHARING.—Nothing in this section may be construed to restrict or condition a non-Federal entity from sharing, for cybersecurity purposes, cyber threat indicators, defensive measures, or information related to cybersecurity risks or incidents with any other non-Federal entity, and nothing in this section may be construed as requiring any non-Federal entity to share cyber threat indicators, defensive measures, or information related to cybersecurity risks or incidents with the Center.

"(I) FEDERAL PREEMPTION.—This section supersedes any statute or other provision of law of a State or political subdivision of a State that

restricts or otherwise expressly regulates an activity authorized under this section.

"(j) DIRECT REPORTING.—The Secretary shall develop policies and procedures for direct reporting to the Secretary by the Director of the Center regarding significant cybersecurity risks and incidents.

"(k) ADDITIONAL RESPONSIBILITIES.—The Secretary shall build upon existing mechanisms to promote a national awareness effort to educate the general public on the importance of securing information systems.

"(l) REPORTS ON INTERNATIONAL COOPERATION.—Not later than 180 days after the date of the enactment of this subsection and periodically thereafter, the Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the range of efforts underway to bolster cybersecurity collaboration with relevant international partners in accordance with subsection (c)(8).

"(m) OUTREACH.—Not later than 60 days after the date of the enactment of this subsection, the Secretary, acting through the Under Secretary for Cybersecurity and Infrastructure Protection, shall—

"(1) disseminate to the public information about how to voluntarily share cyber threat indicators and defensive measures with the Center; and

"(2) enhance outreach to critical infrastructure owners and operators for purposes of such sharing.".

SEC. 4. INFORMATION SHARING AND ANALYSIS ORGANIZATIONS.

Section 212 of the Homeland Security Act of 2002 (6 U.S.C. 131) is amended—

(1) in paragraph (5)—

(A) in subparagraph (A)—

(i) by inserting "information related to cybersecurity risks and incidents and" after "critical infrastructure information"; and

(ii) by striking "related to critical infrastructure" and inserting "related to cybersecurity risks, incidents, critical infrastructure, and";

(B) in subparagraph (B)—

(i) by striking "disclosing critical infrastructure information" and inserting "disclosing cybersecurity risks, incidents, and critical infrastructure information"; and

(ii) by striking "related to critical infrastructure or" and inserting "related to cybersecurity risks, incidents, critical infrastructure, or" and

(C) in subparagraph (C), by striking "disseminating critical infrastructure information" and inserting "disseminating cybersecurity risks, incidents, and critical infrastructure information"; and

(2) by adding at the end the following new paragraph:

"(8) CYBERSECURITY RISK; INCIDENT.—The terms 'cybersecurity risk' and 'incident' have the meanings given such terms in the second section 226 (relating to the National Cybersecurity and Communications Integration Center).".

SEC. 5. STREAMLINING OF DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY AND INFRASTRUCTURE PROTECTION ORGANIZATION.

(a) CYBERSECURITY AND INFRASTRUCTURE PROTECTION.—The National Protection and Programs Directorate of the Department of Homeland Security shall, after the date of the enactment of this Act, be known and designated as the "Cybersecurity and Infrastructure Protection". Any reference to the National Protection and Programs Direc-

torate of the Department in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Cybersecurity and Infrastructure Protection of the Department.

(b) SENIOR LEADERSHIP OF CYBERSECURITY AND INFRASTRUCTURE PROTECTION.—

(1) IN GENERAL.—Subsection (a) of section 103 of the Homeland Security Act of 2002 (6 U.S.C. 113) is amended—

(A) in paragraph (1)—

(i) by amending subparagraph (H) to read as follows:

"(H) An Under Secretary for Cybersecurity and Infrastructure Protection."; and

(ii) by adding at the end the following new subparagraphs:

"(K) A Deputy Under Secretary for Cybersecurity.

"(L) A Deputy Under Secretary for Infrastructure Protection."; and

(B) by adding at the end the following new paragraph:

"(3) DEPUTY UNDER SECRETARIES.—The Deputy Under Secretaries referred to in subparagraphs (K) and (L) of paragraph (1) shall be appointed by

the President without the advice and consent of the Senate.".

(2) CONTINUATION IN OFFICE.—The individuals who hold the positions referred in subparagraphs (H), (K), and (L) of paragraph (1) of section 103(a) the Homeland Security Act of 2002 (as amended and added by paragraph (1) of this subsection) as of the date of the enactment of this Act may continue to hold such positions.

(c) REPORT.—Not later than 90 days after the date of the enactment of this Act, the Under Secretary for Cybersecurity and Infrastructure Protection of the Department of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the feasibility of becoming an operational component, including an analysis of alternatives, and if a determination is rendered that becoming an operational component is the best option for achieving the mission of Cybersecurity and Infrastructure Protection, a legislative proposal and implementation plan for becoming such an operational component. Such report shall also include plans to more effectively carry out the cybersecurity mission of Cybersecurity and Infrastructure Protection, including expediting information sharing agreements.

SEC. 6. CYBER INCIDENT RESPONSE PLANS.

(a) IN GENERAL.—Section 227 of the Homeland Security Act of 2002 (6 U.S.C. 149) is amended—

*(1) in the heading, by striking "**PLAN**" and inserting "**PLANS**";*

(2) by striking "The Under Secretary appointed under section 103(a)(1)(H) shall" and inserting the following:

"(a) IN GENERAL.—The Under Secretary for Cybersecurity and Infrastructure Protection shall"; and

(3) by adding at the end the following new subsection:

"(b) UPDATES TO THE CYBER INCIDENT ANNEX TO THE NATIONAL RESPONSE FRAMEWORK.—The Secretary, in coordination with the heads of other appropriate Federal departments and agencies, and in accordance with the National Cybersecurity Incident Response Plan required under subsection (a), shall regularly update, maintain, and exercise the Cyber Incident Annex to the National Response Framework of the Department.".

(b) CLERICAL AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by amending the item relating to section 227 to read as follows:

"Sec. 227. Cyber incident response plans.".

SEC. 7. SECURITY AND RESILIENCY OF PUBLIC SAFETY COMMUNICATIONS; CYBERSECURITY AWARENESS CAMPAIGN.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.) is amended by adding at the end the following new sections:

"SEC. 230. SECURITY AND RESILIENCY OF PUBLIC SAFETY COMMUNICATIONS.

"The National Cybersecurity and Communications Integration Center, in coordination with the Office of Emergency Communications of the Department, shall assess and evaluate consequence, vulnerability, and threat information regarding cyber incidents to public safety communications to help facilitate continuous improvements to the security and resiliency of such communications.

"SEC. 231. CYBERSECURITY AWARENESS CAMPAIGN.

"(a) IN GENERAL.—The Under Secretary for Cybersecurity and Infrastructure Protection shall develop and implement an ongoing and comprehensive cybersecurity awareness campaign regarding cybersecurity risks and voluntary best practices for mitigating and responding to such risks. Such campaign shall, at a minimum, publish and disseminate, on an ongoing basis, the following:

"(1) Public service announcements targeted at improving awareness among State, local, and tribal governments, the private sector, academia, and stake-

holders in specific audiences, including the elderly, students, small businesses, members of the Armed Forces, and veterans.

"(2) Vendor and technology-neutral voluntary best practices information.

"(b) CONSULTATION.—The Under Secretary for Cybersecurity and Infrastructure Protection shall consult with a wide range of stakeholders in government, industry, academia, and the non-profit community in carrying out this section.".

(b) CLERICAL AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 226 (relating to cybersecurity recruitment and retention) the following new items:

"Sec. 230. Security and resiliency of public safety communications.
"Sec. 231. Cybersecurity awareness campaign.".

SEC. 8. CRITICAL INFRASTRUCTURE PROTECTION RESEARCH AND DEVELOPMENT.

(a) STRATEGIC PLAN; PUBLIC-PRIVATE CONSORTIUMS.—Title III of the Homeland Security Act of 2002 (6 U.S.C. 181 et seq.) is amended by adding at the end the following new section:

"SEC. 318. RESEARCH AND DEVELOPMENT STRATEGY FOR CRITICAL INFRASTRUCTURE PROTECTION.

"(a) IN GENERAL.—Not later than 180 days after the date of enactment of this section, the Secretary, acting

through the Under Secretary for Science and Technology, shall submit to Congress a strategic plan to guide the overall direction of Federal physical security and cybersecurity technology research and development efforts for protecting critical infrastructure, including against all threats. Such plan shall be updated and submitted to Congress every two years.

"(b) CONTENTS OF PLAN.—The strategic plan, including biennial updates, required under subsection (a) shall include the following:

"(1) An identification of critical infrastructure security risks and any associated security technology gaps, that are developed following—

"(A) consultation with stakeholders, including critical infrastructure Sector Coordinating Councils; and

"(B) performance by the Department of a risk and gap analysis that considers information received in such consultations.

"(2) A set of critical infrastructure security technology needs that—

"(A) is prioritized based on the risks and gaps identified under paragraph (1);

"(B) emphasizes research and development of technologies that need to be accelerated due to

rapidly evolving threats or rapidly advancing infrastructure technology; and

"(C) includes research, development, and acquisition roadmaps with clearly defined objectives, goals, and measures.

"(3) An identification of laboratories, facilities, modeling, and simulation capabilities that will be required to support the research, development, demonstration, testing, evaluation, and acquisition of the security technologies described in paragraph (2).

"(4) An identification of current and planned programmatic initiatives for fostering the rapid advancement and deployment of security technologies for critical infrastructure protection, including a consideration of opportunities for public-private partnerships, intragovernment collaboration, university centers of excellence, and national laboratory technology transfer.

"(5) A description of progress made with respect to each critical infrastructure security risk, associated security technology gap, and critical infrastructure technology need identified in the preceding strategic plan required under subsection (a).

"(c) COORDINATION.—In carrying out this section, the Under Secretary for Science and Technology shall coordi-

nate with the Under Secretary for the National Protection and Programs Directorate.

"(d) CONSULTATION.—In carrying out this section, the Under Secretary for Science and Technology shall consult with—

"(1) critical infrastructure Sector Coordinating Councils;

"(2) to the extent practicable, subject matter experts on critical infrastructure protection from universities, colleges, national laboratories, and private industry;

"(3) the heads of other relevant Federal departments and agencies that conduct research and development relating to critical infrastructure protection; and

"(4) State, local, and tribal governments, as appropriate.".

(b) CLERICAL AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 317 the following new item:

"Sec. 318. Research and development strategy for critical infrastructure protection.".

SEC. 9. REPORT ON REDUCING CYBERSECURITY RISKS IN DHS DATA CENTERS.

Not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security shall sub-

mit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the feasibility of the Department of Homeland Security creating an environment for the reduction in cybersecurity risks in Department data centers, including by increasing compartmentalization between systems, and providing a mix of security controls between such compartments.

SEC. 10. ASSESSMENT.

Not later than two years after the date of the enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that contains an assessment of the implementation by the Secretary of Homeland Security of this Act and the amendments made by this Act and, to the extent practicable, findings regarding increases in the sharing of cyber threat indicators, defensive measures, and information relating to cybersecurity risks and incidents at the National Cybersecurity and Communications Integration Center and throughout the United States.

SEC. 11. CONSULTATION.

The Under Secretary for Cybersecurity and Infrastructure Protection shall produce a report on the feasibility of

creating a risk-informed prioritization plan should multiple critical infrastructures experience cyber incidents simultaneously.

SEC. 12. TECHNICAL ASSISTANCE.

The Inspector General of the Department of Homeland Security shall review the operations of the United States Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to assess the capacity to provide technical assistance to non-Federal entities and to adequately respond to potential increases in requests for technical assistance.

SEC. 13. PROHIBITION ON NEW REGULATORY AUTHORITY.

Nothing in this Act or the amendments made by this Act may be construed to grant the Secretary of Homeland Security any authority to promulgate regulations or set standards relating to the cybersecurity of non-Federal entities, not including State, local, and tribal governments, that was not in effect on the day before the date of the enactment of this Act.

SEC. 14. SUNSET.

Any requirements for reports required by this Act or the amendments made by this Act shall terminate on the date that is seven years after the date of the enactment of this Act.

SEC. 15. PROHIBITION ON NEW FUNDING.

No funds are authorized to be appropriated to carry out this Act and the amendments made by this Act. This Act and such amendments shall be carried out using amounts appropriated or otherwise made available for such purposes.

Union Calendar No. 61

114TH CONGRESS
1ST SESSION

H. R. 1731

[Report No. 114–83]

A BILL

To amend the Homeland Security Act of 2002 to enhance multi-directional sharing of information related to cybersecurity risks and strengthen privacy and civil liberties protections, and for other purposes.

APRIL 17, 2015

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed