114TH CONGRESS } HOUSE OF REPRESENTATIVES { REPORT
1st Session } { 114–83

NATIONAL CYBERSECURITY PROTECTION ADVANCEMENT ACT OF 2015

APRIL 17, 2015.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. MCCAUL, from the Committee on Homeland Security, submitted the following

R E P O R T

together with

ADDITIONAL VIEWS

[To accompany H.R. 1731]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 1731) 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, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

49–006

The amendment is as follows:
Strike all after the enacting clause and insert the following:

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 discerning 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 cybersecurity 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 Cooperative 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 Department, 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 consultation 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 report 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 provision 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 Directorate 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 stakeholders 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. 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 coordinate 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 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 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.

PURPOSE AND SUMMARY

The purpose of H.R. 1731 is to amend the Homeland Security Act of 2002 to enhance multi-directional sharing of information related to cybersecurity risks, while strengthening privacy and civil liberties protections, in order to help secure the nation's cyber networks and critical infrastructure against attacks.

BACKGROUND AND NEED FOR LEGISLATION

Despite the growing acknowledgement and understanding of the threat, the U.S. economy and private citizens continue to sustain damage from cyber attacks. The destructive attack on Sony Pictures attributed to the Democratic People's Republic of Korea, and breaches at health insurance providers Anthem and Blue Cross, which compromised sensitive medical records of millions of Americans, are the latest and most prominent examples of intrusions that occur daily, targeting critical infrastructure and business, and victimizing private citizens.

The Department of Homeland Security (Department) estimates that it received nearly 100,000 cyber incident reports, detected 64,000 major vulnerabilities, issued nearly 12,000 alerts or warnings, and responded to 115 major cyber incidents last year alone. It is important to note that these numbers only capture the information reported to the Department. It is fair to say these statistics under-represent the full scope of cyber attacks in the U.S. More-

over, they do not account for threat reporting to other Federal agencies, or incidents that went unreported by the private sector and the public. Still, these numbers provide a powerful illustration of the malicious nature and the persistence of the threats to America's public and private networks, further demonstrating why legislation to help enhance our awareness of the threat through multi-directional information sharing is urgently needed.

At a summit on cybersecurity convened at Stanford University on February 13, 2015, President Obama said that cyberattacks are one of the Nation's most pressing national security, economic and safety issues. He remarked that they are, "hurting American companies and costing American jobs." In his speech, the President said that "there is only one way to defend America from these cyber threats, and that is through government and industry working together, sharing information as true partners."

While the President's Executive Order "Promoting Private Sector Cybersecurity Information Sharing" was a positive step forward, focusing attention on the need for action, Mastercard Chief Executive Officer Ajay Banga rightly concluded, "We need a real legislative solution. An executive action can only take you so far."[1] Mr. Banga also expressed his support for information sharing commenting, "Rather than fight this in individualized groups, there's some merit in joining hands and doing it together."[2] This statement aligns with the goals industry has articulated to the Committee while drafting this legislation.

The National Cybersecurity Protection Advancement Act of 2015 (NCPA Act) will support the Department in its mission to secure cyberspace by facilitating cooperation between the Federal government and the private sector. While there have been many reasons for the lack of cyber threat information sharing in the past, this gap must be addressed to stop criminals, terrorists, and nation states from exploiting our Nation's sensitive intellectual property and personal data. One way to foster greater sharing of timely cyber threat information is to create a mechanism for the sharing of threat information with privacy protections and legal "safe harbors" in which companies can exchange technical data.

The NCPA Act builds on the progress made in the 113th Congress. The National Cybersecurity Protection Act of 2014 codified the Department's National Cybersecurity and Communications Integration Center (NCCIC) to facilitate multi-directional information sharing between the Federal Government and the private sector. As the lead civilian interface for sharing cyber threat information with the government, the NCCIC is uniquely positioned as a sharing hub to integrate information from multiple sources, and use it to provide government agencies and the private sector with actionable information to recognize, prevent and mitigate harm from cyber attacks.

As codified in the Homeland Security Act of 2002, the NCCIC is overseen by the Department's Privacy Office, which is the government's first statutorily established office with a mandate to protect civil rights and liberties. In order to prevent personal information

---

[1] Katie Zezima, "Obama Signs Executive Order on Sharing Cybersecurity Threat Information", Washington Post, February 12, 2015, available at: *http://www.washingtonpost.com/blogs/post-politics/wp/2015/02/12/obama-to-sign-executive-order-on-cybersecurity-threats/*

[2] Ibid

from inadvertently being shared, the NCPA Act ensures that private information is scrubbed twice: first by the entity sharing the information with the NCCIC, and then again by the NCCIC after it is received. These built-in privacy controls at the Department are important factors that make the Department the logical choice for an interface to facilitate cyber information sharing and explain why privacy advocates have expressed support for the NCCIC's role as the lead civilian information-sharing portal.

The NCPA Act authorizes entities to engage in the voluntary exchange of cyber threat information and to conduct network awareness and defensive measures on their own systems. The Act provides liability protections for private entities that conduct network awareness or voluntary shame technical cyber threat information with the another private entity or the NCCIC. Thus, the NCPA Act creates a critical "safe harbor" for private entities, encouraging their participation and cooperation.

In sum, this much-needed Act will help improve the situational awareness of the government and the private sector to ensure that private networks, including critical infrastructure networks, remain reliable and resilient, thereby enhancing the Nation's economic security and safety of the American public.

HEARINGS

No hearings were held on H.R. 1731. However, the Committee held the following oversight hearings.

On February 12, 2015, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "Emerging Threats and Technologies to Protect the Homeland." The Subcommittee received testimony from Mr. Andy Ozment, Assistant Secretary, Office of Cybersecurity and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security; Dr. Huban Gowadia, Director, Domestic Nuclear Detection Office, U.S. Department of Homeland Security; Mr. Joseph Martin, Acting Director, Homeland Security Enterprise and First Responders Group, Science and Technology Directorate, U.S. Department of Homeland Security; Mr. William Noonan, Deputy Special Agent in Charge, Criminal Investigative Division, Cyber Operations Branch, United States Secret Service, U.S. Department of Homeland Security; and Mr. William Painter, Analyst, Government and Finance Division, Congressional Research Service, Library of Congress.

On February 25, 2015, the Committee held a hearing entitled "Examining the President's Cybersecurity Information Sharing Proposal." The Committee received testimony from Hon. Suzanne Spaulding, Under Secretary, National Protection and Programs Directorate, U.S. Department of Homeland Security; Dr. Phyllis Schneck, Deputy Under Secretary, Cybersecurity and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security; and Dr. Eric Fischer, Senior Specialist, Science and Technology, Congressional Research Service, Library of Congress.

On March 4, 2015, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "Industry Perspectives on the President's Cybersecurity Information Sharing Proposal." The Subcommittee received testimony

from Mr. Matthew J. Eggers, Senior Director, National Security and Emergency Preparedness, U.S. Chamber of Commerce; Ms. Mary Ellen Callahan, Jenner & Block and the Former Chief Privacy Officer, U.S. Department of Homeland Security; Mr. Gregory T. Garcia, Executive Director, Financial Services Sector Coordinating Council; and Dr. Martin Libicki, The RAND Corporation.

COMMITTEE CONSIDERATION

The Committee met on April 14, 2015, to consider H.R. 1731, and ordered the measure to be reported to the House with a favorable recommendation, as amended, by voice vote. The Committee took the following actions:

The Committee agreed to H.R. 1731, amended, by voice vote.

The following amendments were offered:

An amendment offered by MR. ROGERS of Alabama (#1) was AGREED TO by voice vote.

In section 3 of the bill, amending the second section 226 of the Homeland Security Act of 2002, in the proposed subsection (i)(3), add at the end a new Subparagraph entitled "(E) Coordinated Vulnerability Disclosure."

An amendment offered by MR. THOMPSON of Mississippi (#2) was AGREED TO by voice vote.

Redesignate section 8 as section 9.

Insert after section 7 a new section entitled "Sec. 8. Assessment."

An amendment offered by MR. THOMPSON of Mississippi (#3) was NOT AGREED TO by a recorded vote of 10 yeas and 15 nays (Roll Call Vote No. 12).

Redesignate section 8 as section 9.

Insert after section 7 a new section entitled "Sec. 8. Sunset."

An amendment offered by MR. RICHMOND (#4) was NOT AGREED TO by a recorded vote of 11 yeas and 16 nays (Roll Call Vote No. 13).

In section 3 of the bill, in the proposed subsection (i) of the second section 226 of the Homeland Security Act of 2002, insert a new paragraph entitled "(8) Liability Exemptions."

An amendment offered by MR. RICHMOND (#5) was NOT AGREED TO by a recorded vote of 12 yeas and 17 nays (Roll Call Vote No. 14).

In section 3 of the bill, in the proposed subsection (i)(8) of the second section 226 of the Homeland Security Act of 2002, strike "or in good faith fails to act based on such sharing,".

In section 3 of the bill, in the proposed subsection (i)(8) of the second section 226 of the Homeland Security Act of 2002, add at the end the a new subparagraph entitled "(E) Rule of Construction."

An amendment offered by MR. RICHMOND (#6) was AGREED TO by voice vote,

Page 11, line 19, strike "and".

Page 11, line 20, strike "(iv)" and insert "(v)".

Page 11, beginning line 20, insert the following:

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

Page 11, line 23, insert "and" after the semicolon.

Page 11, beginning line 24, insert the following:

(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;".

An amendment offered by MR. RICHMOND (#7) was NOT AGREED TO by a recorded vote of 12 yeas and 17 nays (Roll Call Vote No. 15).

In section 3 of the bill, in the proposed Subsection (i)(9)(C) of the second section 226 of the Homeland Security Act of 2002, insert "the discovery of" before "the date of the violation".

An amendment offered by MR. PERRY (#8) was AGREED TO by voice vote.

In section 3 of the bill, amending the second section 226 of the Homeland Security Act of 2002, add at the end a new clause entitled "(j) Direct Reporting."

An amendment offered by MR. KATKO (#9) was AGREED TO by voice vote,

In section 3 of the bill, amending the second section 226 of the Homeland Security Act of 2002, add at the end a new clause entitled "(j) Additional Responsibilities."

An en bloc amendment offered by MR. KEATING (#10) was AGREED TO by voice vote.

Consisting of the following amendments:

An amendment : Redesignate section 8 as section 9.
Insert after section 7 a new section entitled "Sec. 8. Technical Assistance."

An amendment : In section 3(4) of the bill, amending the second section 226 of the Homeland Security Act of 2002, add at the end a new clause entitled "(j) Reports on International Cooperation.

An en bloc amendment offered by MS. MCSALLY (#11) was AGREED TO by voice vote.

Consisting of the following amendments:

An amendment: In section 3 of the bill, amending the second section 226 of the Homeland Security Act of 2002, in subsection (c), in the proposed paragraph (9), insert "and with State and major urban area fusion centers, as appropriate" before the semicolon at the end.
In section 3 of the bill, amending the second section 226 of the Homeland Security Act of 2002, in subsection (c), in the proposed paragraph (10), strike "and" at the end.
In section 3 of the bill, amending the second section 226 of the Homeland Security Act of 2002, in subsection (c), in the proposed paragraph (11), strike the period at the end and insert a semicolon.
In section 3 of the bill, amending the second section 226 of the Homeland Security Act of 2002, in subsection (c), add at the end the following:
"(12) participating, as appropriate, in exercises run by the Department's National Exercise Program; and
"(13) assessing and evaluating consequence, vulnerability, and threat information regarding cyber incidents in coordination with the Office of Emergency Communications of the Department to help facilitate continuous improvements to the security and resiliency of public safety communications."

An amendment: Redesignate section 8 as section 9.
Insert after section 7 a new section entitled "Sec. 8. Cyber Incident Response Plans."

An amendment offered by MRS. WATSON COLEMAN (#12) was AGREED TO by voice vote.

Redesignate section 8 as section 9.
Insert after section 7 a new section entitled "Sec. 8. Cybersecurity Awareness Campaign."

An en bloc amendment offered by MS. JACKSON LEE (#13) was AGREED TO by voice vote.

Consisting of the following amendments:

An amendment: Redesignate section 8 as section 9.Insert after section 7 a new section entitled "Sec. 8. Consultation."

An amendment: Page 10, line 16, after "defensive measures: insert ", analysis".

An amendment: In section 3 of the bill, amending the second section 226 of the Homeland Security Act of 2002, in the proposed subsection (i)(6)(A), add at the end a new clause entitled "(iv) Consultation."

An amendment: Page 11, line 19, insert ", and by striking 'and' at the end" before the semicolon.
Page 11, line 23, insert ", by inserting 'and' after the semicolon at the end" before the semicolon.
Page 11, beginning line 24, insert the following:
(V) by adding at the end the following new subparagraph: "(H) an agency contact for nongovernment entities;".

An amendment offered by MR. RATCLIFFE (#14) was AGREED TO by voice vote.

In section 3 of the bill, amending the second section of 226 of the Homeland Security Act of 2002, in the proposed subsection (i)(8(A), strike "in good faith".
In section 3 of the bill, amending the second section 226 of the Homeland Security Act of 2002, in the proposed subsection (i)(8)(B), strike "in good faith" each place it appears.

An amendment offered by MR. RATCLIFFE (#15) was AGREED TO by voice vote.

In section 2 of the bill, amending the second section 226 of the Homeland Security Act of 2002, in the proposed subsection (i)(7)(B)(i), in subclause (III), strike "and" at the end.
In section 3 of the bill, amending the second section 226 of the Homeland Security Act of 2002, in the proposed subsection (i)(7)(B)(i), in subclause (IV) strike the period at the end and insert ": and".
In section 3 of the bill, amending the second section 226 of the Homeland Security Act of 2002, in the proposed subsection (i)(7)(B)(i), add at the end the following; "(V) may not be used to engage in surveillance or other collection activities for the purpose of tracking an individual's personally identifiable information."

An amendment offered by MR. RATCLIFFE (#16) was AGREED TO by voice vote.

Redesignate section 8 as section 9.
Insert after section 7 a new section entitled "Sec. 8. Critical Infrastructure Protection Research and Development."

An amendment offered by MR. PAYNE (#17) was AGREED TO by voice vote.

In section 3 of the bill, amending the second section 226 of the Homeland Security Act of 2002, add at the end a new clause entitled "(j) Outreach."

An amendment offered by MR. HURD of Texas (#18) was AGREED TO by voice vote.

Page 9, line 14, strike "(I) and insert "(J)".
Page 11, line 7, strike "and".
Page 11, beginning line 8, insert the following:
"(I) an entity that coordinates with small and medium sized businesses; and".

An en bloc amendment offered by *Mr. Langevin* (#19); was AGREED TO by voice vote.

Consisting of the following amendments:

An amendment: in section 3 of the bill, amending the second section 226 of the Homeland Security Act of 2002, in the proposed subsection (i)(1)(A), in the third sentence, strike "and intentionally".

An amendment: In section 3(4) of the bill, amending the second section 226 of the Homeland Security Act of 2002, amend the proposed subsection (g)(1) with a new subsection entitled (1) In General."

An amendment offered by MR, LOUDERMILK (#20) was AGREED TO by voice vote.

Redesignate section 8 as section 9.
Insert after section 7 a new section entitled "Sec. 8. Sunset."

COMMITTEE VOTES

Clause 3(b) of Rule XIII of the Rules of the House of Representatives requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

An amendment offered by MR. THOMPSON OF MISSISSIPPI (#3) was NOT AGREED TO, by a recorded vote of 10 yeas and 15 nays (Roll Call Vote No. 12). The vote was as follows:

COMMITTEE ON HOMELAND SECURITY
ROLL CALL NO. 12
H.R. 1731

Representative	Yea	Nay	Representative	Yea	Nay
Mr. McCaul, Chair.		X	Mr. Thompson of Mississippi, Ranking Member.	X	
Mr. Smith of Texas			Ms. Loretta Sanchez of California		
Mr. King of New York		X	Ms. Jackson Lee	X	
Mr. Rogers of Alabama		X	Mr. Langevin	X	
Mrs. Miller of Michigan		X	Mr. Higgins	X	
Mr. Duncan of South Carolina			Mr. Richmond	X	
Mr. Marino			Mr. Keating		
Mr. Meehan		X	Mr. Payne	X	
Mr. Barletta		X	Mr. Vela	X	
Mr. Perry		X	Mrs. Watson Coleman	X	
Mr. Clawson of Florida		X	Miss Rice	X	
Mr. Katko		X	Mrs. Torres	X	
Mr. Hurd of Texas		X			
Mr. Carter of Georgia		X			
Mr. Walker		X			
Mr. Loudermilk		X			
Ms. McSally		X			
Mr. Ratcliffe		X			
			Vote Total:	**10**	**15**

An amendment offered by MR. RICHMOND (#4) was NOT AGREED TO, by a recorded vote of 11 yeas and 16 nays (Roll Call Vote No. 13). The vote was as follows:

COMMITTEE ON HOMELAND SECURITY
ROLL CALL NO. 13
H.R. 1731

Representative	Yea	Nay	Representative	Yea	Nay
Mr. McCaul, Chair		X	Mr. Thompson of Mississippi, Ranking Member.	X	
Mr. Smith of Texas		X	Ms. Loretta Sanchez of California		
Mr. King of New York		X	Ms. Jackson Lee	X	
Mr. Rogers of Alabama		X	Mr. Langevin	X	
Mrs. Miller of Michigan		X	Mr. Higgins	X	
Mr. Duncan of South Carolina			Mr. Richmond	X	
Mr. Marino			Mr. Keating	X	
Mr. Meehan		X	Mr. Payne	X	

Representative	Yea	Nay	Representative	Yea	Nay
Mr. Barletta		X	Mr. Vela	X	
Mr. Perry		X	Mrs. Watson Coleman	X	
Mr. Clawson of Florida		X	Miss Rice	X	
Mr. Katko		X	Mrs. Torres	X	
Mr. Hurd of Texas		X			
Mr. Carter of Georgia		X			
Mr. Walker		X			
Mr. Loudermilk		X			
Ms. McSally		X			
Mr. Ratcliffe		X			
			Vote Total:	**11**	**16**

An amendment offered by MR. RICHMOND (#5) was NOT AGREED TO, by a recorded vote of 12 yeas and 17 nays (Roll Call Vote No. 14). The vote was as follows:

COMMITTEE ON HOMELAND SECURITY
ROLL CALL NO. 14
H.R. 1731

Representative	Yea	Nay	Representative	Yea	Nay
Mr. McCaul, Chair		X	Mr. Thompson of Mississippi, Ranking Member.	X	
Mr. Smith of Texas		X	Ms. Loretta Sanchez of California	X	
Mr. King of New York		X	Ms. Jackson Lee	X	
Mr. Rogers of Alabama		X	Mr. Langevin	X	
Mrs. Miller of Michigan		X	Mr. Higgins	X	
Mr. Duncan of South Carolina			Mr. Richmond	X	
Mr. Marino		X	Mr. Keating	X	
Mr. Meehan		X	Mr. Payne	X	
Mr. Barletta		X	Mr. Vela	X	
Mr. Perry		X	Mrs. Watson Coleman	X	
Mr. Clawson of Florida		X	Miss Rice	X	
Mr. Katko		X	Mrs. Torres	X	
Mr. Hurd of Texas		X			
Mr. Carter of Georgia		X			
Mr. Walker		X			
Mr. Loudermilk		X			
Ms. McSally		X			
Mr. Ratcliffe		X			
			Vote Total:	**12**	**17**

An amendment offered by MR. RICHMOND (#7) was NOT AGREED TO, by a recorded vote of 12 yeas and 17 nays (Roll Call Vote No. 15). The vote was as follows:

COMMITTEE ON HOMELAND SECURITY
ROLL CALL NO. 15
H.R. 1731

Representative	Yea	Nay	Representative	Yea	Nay
Mr. McCaul, Chair		X	Mr. Thompson of Mississippi, Ranking Member.	X	
Mr. Smith of Texas		X	Ms. Loretta Sanchez of California	X	
Mr. King of New York		X	Ms. Jackson Lee	X	
Mr. Rogers of Alabama		X	Mr. Langevin	X	
Mrs. Miller of Michigan		X	Mr. Higgins	X	
Mr. Duncan of South Carolina			Mr. Richmond	X	
Mr. Marino		X	Mr. Keating	X	
Mr. Meehan		X	Mr. Payne	X	
Mr. Barletta		X	Mr. Vela	X	
Mr. Perry		X	Mrs. Watson Coleman	X	
Mr. Clawson of Florida		X	Miss Rice	X	
Mr. Katko		X	Mrs. Torres	X	
Mr. Hurd of Texas		X			
Mr. Carter of Georgia		X			
Mr. Walker		X			
Mr. Loudermilk		X			
Ms. McSally		X			
Mr. Ratcliffe		X			
			Vote Total:	**12**	**17**

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of Rule XIII of the Rules of the House of Representatives, the Committee has held oversight hearings and made findings that are reflected in this report.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of Rule XIII of the Rules of the House of Representatives, the Committee finds that H.R. 1731, the National Cybersecurity Protection Advancement Act of 2015, would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, April 16, 2015.

Hon. MICHAEL MCCAUL,
Chairman, Committee on Homeland Security,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 1731, the National Cybersecurity Protection Advancement Act of 2015.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Jason Wheelock.

Sincerely,

KEITH HALL,
Director.

Enclosure.

H.R. 1731—National Cybersecurity Protection Advancement Act of 2015

H.R. 1731 would largely codify the role of the National Cybersecurity and Communications Integration Center of the Department of Homeland Security in exchanging information about cyber threats with other federal agencies and nonfederal entities. The legislation also would require that certain additional procedures be followed when that information is shared, such as checking for and expunging personal information. Finally, the bill would require several reports to the Congress on cybersecurity information sharing. CBO anticipates that approximately 20 additional personnel would be needed to administer the new aspects of the program, prepare the required reports, and manage the exchange of information. Based on information from the Department of Homeland Security, the Office of Management and Budget, and other cybersecurity experts, CBO estimates that the requirements imposed by H.R. 1731 would cost approximately $20 million over the 2016–2020 period, assuming appropriation of the estimated amounts.

H.R. 1731 would make the government liable if an agency or department violates privacy and civil liberty guidelines and restrictions on the use of information required by the bill. While such liability could result in additional direct spending, CBO does not have sufficient basis to estimate the type or frequency of violations or the budgetary effect that might occur if the legislation was enacted. Because the bill could affect direct spending, pay-as-you-go procedures apply. H.R. 1731 would not affect revenues.

H.R. 1731 would impose intergovernmental and private-sector mandates, as defined in the Unfunded Mandates Reform Act (UMRA), by extending civil and criminal liability protection to cybersecurity providers and other entities that monitor, share, or use information on cyber threats. Doing so would prevent public and private entities from seeking compensation for damages from those protected entities for sharing or using cybersecurity information. The bill also would impose additional intergovernmental mandates on state and local governments by preempting disclosure and liability laws and by preempting any laws that restrict the cybersecurity monitoring, sharing, and countermeasure activities authorized by the bill. Because of uncertainty about the number of cases that would be limited and any foregone compensation that would result from compensatory damages that might otherwise go to private-sector entities, CBO cannot determine whether the costs of the mandate would exceed the annual thresholds established in UMRA for private-sector mandates ($154 million in 2015, adjusted annually for inflation). The amount of cybersecurity information shared by state, local, and tribal governments is much smaller than that shared by the private sector, and public entities are much less likely to bring lawsuits as plaintiffs in such cases. Consequently, CBO estimates that the aggregate costs of the mandates on public entities would fall below the threshold for intergovernmental mandates ($77 million in 2015, adjusted annually for inflation).

On April 13, 2015, CBO transmitted a cost estimate for H.R. 1560 as ordered reported by the House Permanent Select Committee on Intelligence on March 26, 2015, and on April 14, 2015,

CBO transmitted a cost estimate for S. 754 as reported by the Senate Select Committee on Intelligence on March 17, 2015. Both bills are similar to H.R. 1731, but each contains provisions not included in H.R. 1731 that would allow the government to use information shared by nonfederal entities in investigating and prosecuting certain violent crimes. In addition, H.R. 1560 contains a provision not included in H.R. 1731 that would establish a National Cyber Threat Intelligence Integration Center. Differences in the estimated costs of these bills reflect differences in the legislative language.

The CBO staff contact for this estimate is Jason Wheelock. The estimate was approved by Theresa Gullo, Assistant Director for Budget Analysis.

Statement of General Performance Goals and Objectives

Pursuant to clause 3(c)(4) of Rule XIII of the Rules of the House of Representatives, H.R. 1731 contains the following general performance goals and objectives, including outcome related goals and objectives authorized.

H.R. 1731 seeks to enhance multi-directional sharing of information related to cybersecurity risks, while also strengthening privacy and civil liberties protections, in order to help secure the nation's cyber networks and critical infrastructure against attacks. The legislation requires a number of reports to Congress from the Department, the Department's Privacy Officer, and the Department's Office of Inspector General that will provide insight to Congress on the scope of information sharing, the NCCIC's role in facilitating cyber information sharing, and any privacy and civil liberties concerns that have been raised as a result of this effort.

Duplicative Federal Programs

Pursuant to clause 3(c) of Rule XIII, the Committee finds that H.R. 1731 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

Congressional Earmarks, Limited Tax Benefits, and Limited Tariff Benefits

In compliance with Rule XXI of the Rules of the House of Representatives, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(e), 9(f), or 9(g) of the Rule XXI.

Federal Mandates Statement

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

Preemption Clarification

In compliance with section 423 of the Congressional Budget Act of 1974, requiring the report of any Committee on a bill or joint resolution to include a statement on the extent to which the bill or joint resolution is intended to preempt State, local, or Tribal law,

the Committee finds that H.R. 1731 does preempt all State, local, or Tribal law that restricts or otherwise expressly regulates an activity that is authorized under this legislation with respect to a Federal civilian cybersecurity information sharing program.

DISCLOSURE OF DIRECTED RULE MAKINGS

The Committee estimates that H.R. 1731 would require no directed rule makings.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short Title.

This section provides that the bill may be cited as the "National Cybersecurity Protection Advancement Act of 2015."

Section 2. National Cybersecurity and Communications Integration Center.

This section amends subsection (a) of the second section 226 (6 U.S. Code 148) of the Homeland Security Act of 2002 by adding definitions of terms used in the bill, including: "cyber threat indicator", "cybersecurity purpose", "defensive measure", "network awareness", "private entity", "security control", and "sharing".

Section 3. Information Sharing Structure and Process.

This section amends subsection (a) of the second section 226 of the Homeland Security Act of 2002 as described below.

Amendments to the National Cybersecurity and Communications Integration Center.

This section amends the functions of the NCCIC. It designates the NCCIC as the "lead Federal civilian interface" for multi-directional and cross-sector information sharing related to cybersecurity.

It also adds cyber threat indicators and defensive measures to the types of technical threat data that the NCCIC will collect, analyze, and share to provide enhanced situational awareness to Federal, non-Federal and private entities. It directs the NCCIC to share information relating to cybersecurity risks and incidents with small and medium-sized businesses, as appropriate. The Committee believes that the NCCIC should strive to partner with small and medium-sized businesses for cybersecurity risks and incidents, and seeks to emphasize this in the legislation.

It directs the NCCIC to promptly notify the Secretary of Homeland Security (the Secretary) and Congress of any significant violations of information sharing policies and procedures, and promptly

notify non-Federal entities that have shared information that is known or determined to be in error. The Committee understands that certain entities have pre-existing relationships with other Federal civilian portals representing their specific critical infrastructure sectors, and those entities will be able to maintain those relationships for information sharing related to cybersecurity. As the lead civilian interface for sharing cyber threat information with the Government, the NCCIC is uniquely positioned as a sharing hub to integrate information from multiple sources, and use the information to Government Agencies and the private sector with actionable information to recognize and stop attacks before harm is done.

The Committee believes that the NCCIC should coordinate with other Federal civilian portals to ensure that it receives and shares relevant cyber threat indicators and defensive measures.

This section directs the NCCIC to engage with international partners on cybersecurity, and expands the composition of the NCCIC to include an entity to collaborate with state and local governments; the U.S. Computer Emergency Readiness Team to coordinate information related to cybersecurity risks and incidents and provide technical assistance; the Industrial Control System Cyber Emergency Response Team to coordinate with industrial control systems owners and operators; and the National Coordinating Center for Communications to coordinate the resilience and recovery of national security emergency communications. The Committee recognizes that the entities described above play a critical role in the Department's ability to execute its cybersecurity mission, and seeks to codify their functions and statutory roles within the NCCIC in this section.

H.R. 1731 amends second section 226, the provisions of which are described below:

(g) Rapid Automated Sharing.

This subsection requires the Under Secretary for Cybersecurity and Infrastructure Protection, in coordination with industry and other stakeholders, to develop an automated capability for the timely sharing of cyber threat indicators and defensive measures. It also directs the NCCIC to develop the capability to share cyber threat indicators and defensive measures with each Federal Agency designated as the 'Sector Specific Agency' (SSA) for each critical infrastructure sector in as close to real time as practicable. It directs the Under Secretary for Cybersecurity and Infrastructure Protection to submit a biannual report to the appropriate congressional committees on the progress of developing this capability. The Committee believes that it is critical for the Department to develop an automated system and supporting processes for the NCCIC to disseminate cyber threat indicators and defensive measures in a timely manner. The Committee recognizes that timely sharing is compatible with reasonable efforts at minimization, particularly if the information shared is cyber threat indicator information.

(h) Sector Specific Agencies

This subsection directs the Secretary to recognize the SSA for each critical infrastructure sector based on the Department's National Infrastructure Protection Plan as of March 25, 2015. It directs the Secretary, in coordination with the heads of each SSA, to

support the security and resilience activities of the specific sectors, provide institutional knowledge and expertise, and support timely sharing of information. The Committee believes that SSAs play a central role in cybersecurity information sharing within their respective sector and wants to ensure that the NCCIC has the procedures and capabilities in place to facilitate information sharing with each SSA.

(i) Voluntary Information Sharing Procedures

Subsection (i) outlines the information sharing procedures and permits the NCCIC to enter into voluntary information sharing relationships with any consenting non-Federal entity for the sharing of cyber threat indicators and defensive measures for cybersecurity purposes. To prevent personal information from inadvertently being shared, the non-Federal entity sharing the information is required to remove all personal information unrelated to the cybersecurity risk before sharing with the NCCIC or other non-Federal entities. This subsection outlines the information sharing agreements, authorizations, civil liberty and information protections, and antitrust exemption of these relationships.

The Committee believes that sharing cybersecurity information is a voluntary decision. In order to encourage the sharing of cybersecurity information to secure the nation's cyber networks and critical infrastructure against attacks, the Committee believes that any non-Federal entity can voluntarily enter into an information sharing relationship with the NCCIC. This relationship is dependent on adherence to information protection and privacy and civil liberties protections, in return for receiving a legal "safe harbor" for appropriately sharing technical data about cyber threat indicators and defensive measures. The Committee believes technical data to mean the specific composition, or the "bits and bytes," that make up cyber threat indicators and defensive measures.

(2) Agreements

Subsection (i)(2) allows the Center to utilize standard and negotiated agreements as the types of agreements that non-Federal entities may enter into with the NCCIC for the purposes of this Act. However, it makes clear that agreements are not limited to just these types, and pre-existing agreements between the NCCIC and the non-Federal entity will be in compliance with this section.

The Committee believes that there are various ways to structure agreements, with the primary types being standard and negotiated agreements. The Department should develop a standard template that will inform entities on the expectations and requirements of sharing cybersecurity information with the NCCIC. It may turn out that, in some cases, standardized terms of use agreements will suffice. However, for those entities that have specific requirements, they should be able to negotiate with the Department on specific terms, so long as foundational privacy protections are maintained. Due to the fact information sharing under this Act is a voluntary activity, the Committee also recognizes that an entity may not feel the need to have any agreement with the NCCIC, but may still want to share cybersecurity information.

(3) Information Sharing Authorization

Subsection (i)(3) authorizes a non-Federal entity to share cyber threat indicators or defensive measures obtained from its own information system or, with written consent, from an information system of another Federal or non-Federal entity, with another non-Federal entity and the NCCIC for cybersecurity purposes. It requires that recipients of this information comply with lawful restrictions on sharing or use. It also requires a recipient of information from another Federal or non-Federal entity to comply with lawful restrictions placed on the information by the sharing Federal or non-Federal entity.

This subsection also requires the Under Secretary for Cybersecurity and Infrastructure Protection, in coordination with industry and other stakeholders to develop and adhere to policies and procedures for coordinating vulnerability disclosures, to the extent practicable, with international standards in the information technology industry.

The Committee believes that in order to facilitate robust information sharing, non-Federal entities need the right to place lawful restrictions on the use of the technical data they are sharing, and that these restrictions must be respected by the recipients of the information.

This subsection also requires a non-Federal entity to take reasonable efforts to remove information that could be used to identify specific persons reasonably believed at the time of sharing to be unrelated to a cybersecurity threat, and safeguard information that can be used to identify specific persons from unintended disclosure and unauthorized access or acquisition.

The Committee's intent in this section is to specifically forbid non-Federal entities from sharing data that has not had personal information unrelated to the cybersecurity risk removed by the non-Federal entity prior to sharing. Additionally, the NCCIC is required to review the same cybersecurity threat indicator or defensive measure information and destroy any personal information unrelated to the cybersecurity risk prior to sharing with any other Federal or non-Federal entity.

The purpose of this legislation is to secure the nation's cyber networks and private citizen's sensitive digital information. The Committee believes that in order to ensure that privacy is protected when cyber security information is shared, and to build trust in this effort, the public must feel confident that companies and the government have robust controls in place to remove any specific personal information not related to the cyber attack, and safeguard it from unintended disclosure and unauthorized use or acquisition.

(4) Network Awareness Authorization

Subsection (i)(4) authorizes a non-Federal entity, not including a State, local, or Tribal government, to conduct network awareness of its own information system, or the information system of another non-Federal or Federal entity with written consent, for cybersecurity purposes.

(5) Defensive Measure Authorization

Subsection (i)(5) authorizes a non-Federal entity, not including a State, local, or Tribal government, to conduct network awareness

defensive measure that is applied only to its own information system, or the information system of another non-Federal or Federal entity with written consent, for cybersecurity purposes.

The Committee does not intend the language of the Act to authorize a private company to "hack" (knowingly access a protected computer without authorization, or to intentionally access a protected computer to cause damage) the computer of another entity.

The intent is only to authorize the use of defensive measures—not countermeasures. This authorization does not allow a measure that destroys, renders unusable, or substantially harms an information system not belonging to that company without authorization.

(6) Privacy and Civil Liberties Protections

Subsection (i)(6) requires the Under Secretary in coordination with the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties at the Department to establish and annually review policies and procedures for the Department that govern the receipt, retention, use, and disclosure of cyber threat indicators and information related to cybersecurity risks and incidents.

This subsection requires that certain policies and procedures to minimize any impact on privacy and civil liberties should be established consistent with the need to protect information systems from, and conduct mitigation of, cybersecurity risks and incidents in a timely manner.

The subsection requires the Chief Privacy Officer to submit a report to the appropriate congressional committees, no later than 180 days after enactment of this Act, that describes the policies and procedures governing the sharing of cyber threat indicators and defensive measures. The subsection also requires the Chief Privacy Officer to monitor the implementation of these policies and procedures, and regularly review and update privacy impact assessments to ensure all relevant constitutional, legal, and privacy protections are being followed. The subsection further requires the Chief Privacy Officer to submit an annual report to Congress on the effectiveness of these policies and procedures, ensuring appropriate sanctions are in place for employees, agents, and contractors of the Department who intentionally or willfully conduct unauthorized activities under this section.

Additionally, the subsection requires the Undersecretary to ensure that a public notice is made of the policies and procedures governing the sharing of cyber threat indicators and defensive measures.

This subsection requires the Department's Office of the Inspector General (DHS OIG) to submit a report to Congress within two years of enactment of this Act and periodically thereafter that includes a review of the type of information shared with NCCIC, the use of any information and actions taken by NCCIC, and the impact, if any, of sharing of such information on privacy and civil liberties.

This subsection requires that the Department's Chief Privacy Officer and Officer for Civil Rights and Civil Liberties also submit a report to Congress within two years of enactment of this Act that assesses the impact on privacy and civil liberties of the information sharing activities under this section. The report shall include ap-

propriate recommendations to minimize or mitigate the impact of the sharing of cyber threat indicators and defensive measures under this section.

The Committee believes that this legislation strengthens the NCCIC's position as the trusted partner for industry and the public by setting forth robust privacy protections and civil liberties standards. To ensure the appropriate protection of individual privacy and civil liberties, the Department's Privacy and Civil Rights and Civil Liberties Offices will monitor the NCCIC as it carries out its functions. The Committee believes that the required reports in this subsection will assist the Department in defining the policies and procedures for the sharing of cyber threat indicators and defensive measures with the NCCIC, and provide Congress with assessments on the impact to privacy and civil liberties of this information sharing.

The Committee believes that privacy is further reinforced by requiring non-Federal entities to remove personal information unrelated to a cybersecurity risk or incident before sharing with the NCCIC or other non-Federal entities, and further requiring the NCCIC to destroy any personal information that is unrelated to the cybersecurity risk or incident before further sharing with other Federal entities or non-Federal entities.

(7) Uses and Protection of Information

This subsection sets forth the roles and responsibilities for non-Federal entities, Federal entities, and State, Tribal, and local governments for using and protecting information shared through the NCCIC or otherwise.

Non-Federal Entities

Subsection (i)(7) permits a non-Federal entity that shares cybersecurity information with the NCCIC, or another non-Federal entity, to use, retain, or disclose those cyber threat indicators and defensive measures solely for cybersecurity purposes. It requires non-Federal entities to remove information that could be used to identify specific persons reasonably believed at the time of sharing to be unrelated to a cybersecurity threat and safeguard information that can be used to identify specific persons prior to sharing the information. Non-Federal entities must comply with appropriate restrictions placed on the subsequent disclosure or retention of cyber threat indicators or defensive measures by a Federal or non-Federal entity. This subsection further stipulates that information shared with the NCCIC will be deemed to have been voluntarily shared. This subsection requires that a non-Federal entity implements and utilizes a security control to protect against unauthorized access to or acquisition of cyber threat indicators or defensive measures, and it prohibits the use of such cyber security information to gain an unfair or competitive advantage over any non-Federal entity.

Federal Entities

This subsection permits Federal entities that receive cyber threat indicators or defensive measures to use, retain, or further disclose this information solely for cybersecurity purposes. This subsection requires Federal entities to take reasonable to efforts to remove in-

formation that could be used to identify specific persons reasonably believed at the time of sharing to be unrelated to a cybersecurity threat and safeguard information that can be used to identify specific persons prior to sharing the information. This subsection further stipulates that information shared with the NCCIC will be deemed to have been voluntarily shared. This subsection requires that a Federal entity implements and utilizes a security control to protect against unauthorized access to or acquisition of cyber threat indicators or defensive measures.

The cybersecurity information is exempt from disclosure under the Freedom of Information Act (FOIA), 5 U.S. Code 552, or non-Federal disclosure laws and withheld, without discretion, from the public under 5 U.S. Code 552(3)B). This subsection allows a Federal or non-Federal entity to designate information shared with the Center as commercial, financial, and proprietary information. The information shared is prohibited from being used for regulatory purposes, and may not constitute a waiver of applicable privileges or protections provided by law, including trade secret protections. The information is also not subject to judicial doctrine or rules of federal entities regarding ex parte communications.

The Committee believes that in order to encourage entities, particularly businesses, to voluntarily share cybersecurity information with the NCCIC, the information shared must be exempt from disclosure laws including FOIA, and be prohibited from being used for regulatory purposes. The Committee believes that it is also within the right of the entity sharing the information to put certain restrictions on how the information maybe used or further shared, as articulated in the legislation.

The Committee intends this to be a private sector-driven program. The government itself will not conduct any network monitoring. The NCCIC is simply a repository, a hub, for threat information that is identified by private entities and voluntarily shared with the government.

The sole purpose of the activities codified in this legislation is to prevent cyber attacks—*e.g.* the stealing of credit card numbers; the shutting down of infrastructure, like a power grid; the shutting down of a network—not to collect evidence to prosecute crimes.

State, Tribal, or Local Government

This subsection permits State, Tribal or local governments that receive cyber threat indicators or defensive measures to use, retain, or further disclose this information solely for cybersecurity purposes. It requires prior to sharing that reasonable efforts be made to remove information that could be used to identify specific persons reasonably believed to be unrelated to a cybersecurity threat and safeguard information that can be used to identify specific persons prior to sharing the information. This subsection allows a Federal or non-Federal entity to designate information shared with the Center as commercial, financial, and proprietary information. This subsection further stipulates that information shared with the NCCIC will be deemed to have been voluntarily shared. This subsection requires that a State, Tribal or local government implement and utilize security controls to protect against unauthorized access to or acquisition of cyber threat indicators or defensive measures. This subsection states that cybersecurity information is exempt

from disclosure under State, Tribal or local disclosure laws, and may not be used to regulate the lawful activity of a non-Federal entity.

The Committee believes it is important to re-emphasize that prior to sharing entities remove information that can be used to identity specific persons and is reasonably believed at the time of sharing to be unrelated to a cybersecurity risk or incident. Cybersecurity information that is shared with the NCCIC would then be reviewed again prior to the NCCIC sharing it with another entity, to ensure that personal information is removed.

In this section, the Committee expressly states that cyber threat indicators and defensive measures may not be used to track individuals for purposes of surveillance. Again, the purpose of this legislation is to help prevent and respond to cyber attacks—not to surveil individuals, or collect evidence to prosecute crimes.

(8) Liability Exemptions

Subsection (i)(8) provides that 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 conducts network awareness or shares cyber threat indicators or defensive measures, for cybersecurity purposes, in accordance with paragraphs (4) and (3), respectively, and the other provisions in section 3 of the bill. This subsection also provides liability protection for a non-Federal entity that fails to act upon shared cyber threat indicators or defensive measures.

However, non-Federal entities do not receive liability protection for egregious actions that rise to the level of willful misconduct. Willful misconduct is defined in the subsection as an act or omission that is taken intentionally to achieve a wrongful purpose, knowingly without legal or factual justification, and 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. If a plaintiff files suit claiming willful misconduct by a non-Federal entity, the plaintiff must prove willful misconduct by clear and convincing evidence and establish that the non-Federal entity's willful misconduct proximately caused the plaintiff's injury.

As used in this paragraph, the term "non-Federal entity" does not include a State, local, or tribal government.

This language was developed in coordination with the House Judiciary Committee, which provided standard language for liability exemptions for all House-generated cybersecurity related information sharing bills.

(9) Federal Government Liability for Violations of Restrictions on the Use and Protection of Voluntarily Shared Information

Subsection (i)(9) provides a clear path for injured persons to sue a Federal government department or agency for an intentional or willful violation of the uses and protections of voluntarily shared cyber threat indicators, defensive measures, or cybersecurity information as laid out in subsections (i)(3), (i)6), and (i)(7)(B), and any other applicable provisions of section 3. This subsection further provides for statutory damages for such a violation, venue selection

for an action under this provision, and the statute of limitations for bringing such an action.

(10) Anti-Trust Exemption

This subsection exempts non-Federal entities from violations of U.S. antitrust law for sharing cybersecurity information, or providing assistance for cybersecurity purposes, provided that the action is taken to assist with preventing, investigating, or mitigating a cybersecurity risk or incident. This subsection makes it clear that the exemption cannot be utilized for monopolistic activities such as price-fixing, or sharing of price or cost information, customer lists, or information regarding future planning.

(11) Construction and Preemption

Subsection (i)(11) contains a number of construction and preemption provisions that address the scope of the Act. Specifically, the provisions address otherwise lawful disclosures and preserve whistleblower protections. Nothing in the Act should be construed to affect any requirements under other provisions of law for non-Federal entities providing information to Federal entities. The provisions preserve existing contractual obligations and rights. They also prohibit the Federal government from requiring non-Federal entities to provide it with cybersecurity related information as a condition for the award of a grant, contract or purchase agreement. This subsection reiterates that any sharing of cybersecurity information under this legislation is purely voluntary, and that non-Federal entities are not subject to liability for choosing not to engage in such voluntary information sharing activities. This subsection also does not authorize or modify any existing Federal authority to retain and use cybersecurity information shared under the bill for purposes other than those permitted in this Act. This legislation also supersedes any provision of state or local law that may restrict or otherwise expressly regulate an activity authorized under this Act.

Section 4. Information Sharing and Analysis Organizations.

This section amends Section 212 of the Homeland Security Act to broaden the functions of Information Sharing and Analysis Organizations (ISAOs) to include cybersecurity risk and incident information beyond that pertaining to critical infrastructure. This section also adds references to the definitions of 'cybersecurity risk' and 'incident' as they relate to the NCCIC in the second section 226 of the Homeland Security Act.

The Committee believes that ISAOs have an important role to play in facilitating information sharing going forward and has clarified their functions as defined in the Homeland Security Act. The Committee, on a bipartisan basis, views ISAOs, including ISACs as tools to expand voluntary information sharing.

Section 5. Streamlining of Department of Homeland Security Cybersecurity and Infrastructure Protection Organization.

This section renames The National Protection and Programs Directorate of the Department of Homeland Security, the "Cybersecurity and Infrastructure Protection Directorate". It requires the Secretary to submit a report to Congress on the feasibility of making

the Cybersecurity and Communications Office an operational component of the Department. The Committee is pleased that this legislation elevates the role of the NCCIC to a direct report to the Assistant Secretary of Cybersecurity and Communications within the Department. The Committee believes this re-organization aligns with its goals to reduce the bureaucracy that has stifled the NCCIC's growth to date.

Nothing in this section should be construed to alter the mission or reporting structure of the Office of Emergency Communications. Pursuant to 6 U.S.C. 571, the Director of the Office of Emergency Communications reports to the Assistant Secretary for Cybersecurity and Communications. The Department shall submit any proposed changes to this reporting structure to the Committee for review and approval.

Section 6. Cyber Incident Response Plans.

This section requires the Secretary, in coordination with the heads of other Federal departments and agencies to update, maintain, and exercise the Cyber Incident Annex to the National Response Framework of the Department.

Section 7. Security and Resiliency of Public Safety Communications; Cybersecurity Awareness Campaign.

This section requires the NCCIC, in coordination with the Office of Emergency Communications, to assess the effects of cyber incidents on public safety communications.

This section also requires the Under Secretary for Cybersecurity and Infrastructure Protection to develop and implement a cybersecurity awareness campaign regarding cybersecurity risks and voluntary best practices for mitigating and responding to cybersecurity risks.

The Committee has observed the perceived inadequacy of the Department's current cybersecurity awareness campaign, STOP. THINK. CONNECT.™ While the Department and a coalition of private companies, non-profits and government organizations developed and coordinated this message, purported to help all digital citizens stay safer and more secure online, the Committee feels there needs to be a renewed effort to use and target more widely used media and public knowledge bases.

The Committee believes that the Department should put out effective Public Service announcements, widely advertised web sites, apps, written collateral, social media, and other creative sources to help folks understand that many simple measures will improve their cyber security protection posture. The Committee believes that the Department should be offering specific information, not just slogans, and advising where to get information along with technology-neutral best practices, and working with a wide range of stakeholders to get it done. Such measures include simple steps like: improving password management; enabling firewall protection; installing anti-virus and anti-spam protection; installing software updates; and refrain from opening links and attachments from unknown and untrusted senders.

Section 8. Critical Infrastructure Protection Research and Development.

This section requires the Secretary, acting through the Under Secretary for Science and Technology, to submit a strategic plan to Congress within 180 days for guiding the direction of Federal physical security and cybersecurity technology research and development efforts for protecting critical infrastructure against all threats.

Section 9. Report on Reducing Cybersecurity Risks in DHS Data Centers.

This section requires the Secretary to submit a report to Congress on the feasibility of the Department creating an environment for the reduction of cybersecurity risks at the Department's data centers.

Section 10. Assessment.

This section requires the Comptroller General of the United States to submit a report to Congress assessing the implementation of this Act no later than two years after the date of enactment of this Act.

Section 11. Consultation.

This section requires the Under Secretary for Cybersecurity and Infrastructure Protection to produce a report on the feasibility of creating a risk-informed plan should multiple critical infrastructure sectors experience cyber incidents simultaneously.

Section 12. Technical Assistance.

This section requires the Inspector General of the Department to 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 their capacity to provide technical assistance to non-Federal entities.

Section 13. Prohibition on New Regulatory Authority.

This section clarifies that nothing in this Act shall be construed to grant the Secretary any authority to promulgate regulations or set standards relating to the cybersecurity of non-Federal entities, not including State, local, or Tribal governments.

Section 14. Sunset.

This section requires that any reporting requirements required by this Act terminate seven years after the date of enactment of this Act.

Section 15. Prohibition on New Funding.

This section states that no new funds are authorized to be appropriated to carry out this Act.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omit-

ted is enclosed in black brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Homeland Security Act of 2002".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

* * * * * * *

* * * * * * *

TITLE I—DEPARTMENT OF HOMELAND SECURITY

* * * * * * *

SEC. 103. OTHER OFFICERS.

(a) DEPUTY SECRETARY; UNDER SECRETARIES.—(1) IN GENERAL.—Except as provided under paragraph (2), there are the following officers, appointed by the President, by and with the advice and consent of the Senate:

(A) A Deputy Secretary of Homeland Security, who shall be the Secretary's first assistant for purposes of subchapter III of chapter 33 of title 5, United States Code.

(B) An Under Secretary for Science and Technology.

(C) An Under Secretary for Border and Transportation Security.

(D) An Administrator of the Federal Emergency Management Agency.

(E) A Director of the Bureau of Citizenship and Immigration Services.

(F) An Under Secretary for Management.

(G) A Director of the Office of Counternarcotics Enforcement.

[(H) An Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department.]

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

(I) Not more than 12 Assistant Secretaries.

(J) A General Counsel, who shall be the chief legal officer of the Department.

(K) A Deputy Under Secretary for Cybersecurity.

(L) A Deputy Under Secretary for Infrastructure Protection.

(2) ASSISTANT SECRETARIES.—If any of the Assistant Secretaries referred to under paragraph (1)(I) is designated to be the Assistant Secretary for Health Affairs, the Assistant Secretary for Legislative Affairs, or the Assistant Secretary for Public Affairs, that Assistant Secretary shall be appointed by the President without the advice and consent of the Senate.

(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.

(b) INSPECTOR GENERAL.—There shall be in the Department an Office of Inspector General and an Inspector General at the head of such office, as provided in the Inspector General Act of 1978 (5 U.S.C. App.).

(c) COMMANDANT OF THE COAST GUARD.—To assist the Secretary in the performance of the Secretary's functions, there is a Commandant of the Coast Guard, who shall be appointed as provided in section 44 of title 14, United States Code, and who shall report directly to the Secretary. In addition to such duties as may be provided in this Act and as assigned to the Commandant by the Secretary, the duties of the Commandant shall include those required by section 2 of title 14, United States Code.

(d) OTHER OFFICERS.—To assist the Secretary in the performance of the Secretary's functions, there are the following officers, appointed by the President:

(1) A Director of the Secret Service.

(2) A Chief Information Officer.

(3) An Officer for Civil Rights and Civil Liberties.

(4) A Director for Domestic Nuclear Detection.

(f) PERFORMANCE OF SPECIFIC FUNCTIONS.—Subject to the provisions of this Act, every officer of the Department shall perform the functions specified by law for the official's office or prescribed by the Secretary.

(e) CHIEF FINANCIAL OFFICER.—There shall be in the Department a Chief Financial Officer, as provided in chapter 9 of title 31, United States Code.

TITLE II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

* * * * * * *

Subtitle B—Critical Infrastructure Information

* * * * * * *

SEC. 212. DEFINITIONS.

In this subtitle:

(1) AGENCY.—The term "agency" has the meaning given it in section 551 of title 5, United States Code.

(2) COVERED FEDERAL AGENCY.—The term "covered Federal agency" means the Department of Homeland Security.

(3) CRITICAL INFRASTRUCTURE INFORMATION.—The term "critical infrastructure information" means information not customarily in the public domain and related to the security of critical infrastructure or protected systems—

(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

(B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or

(C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

(4) CRITICAL INFRASTRUCTURE PROTECTION PROGRAM.—The term "critical infrastructure protection program" means any component or bureau of a covered Federal agency that has been designated by the President or any agency head to receive critical infrastructure information.

(5) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term "Information Sharing and Analysis Organization" means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of—

(A) gathering and analyzing critical infrastructure information *information related to cybersecurity risks and incidents and* in order to better understand security problems and interdependencies **[**related to critical infrastructure**]** *related to cybersecurity risks, incidents, critical infrastructure, and* and protected systems, so as to ensure the availability, integrity, and reliability thereof;

(B) communicating or **[**disclosing critical infrastructure information**]** *disclosing cybersecurity risks, incidents, and critical infrastructure information* to help prevent, detect,

mitigate, or recover from the effects of a interference, compromise, or a incapacitation problem [related to critical infrastructure or] *related to cybersecurity risks, incidents, critical infrastructure, or* protected systems; and

(C) voluntarily [disseminating critical infrastructure information] *disseminating cybersecurity risks, incidents, and critical infrastructure information* to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).

(6) PROTECTED SYSTEM.—The term "protected system"—

(A) means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure; and

(B) includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.

(7) VOLUNTARY.—

(A) IN GENERAL.—The term "voluntary", in the case of any submittal of critical infrastructure information to a covered Federal agency, means the submittal thereof in the absence of such agency's exercise of legal authority to compel access to or submission of such information and may be accomplished by a single entity or an Information Sharing and Analysis Organization on behalf of itself or its members.

(B) EXCLUSIONS.—The term "voluntary"—

(i) in the case of any action brought under the securities laws as is defined in section 3(a)(47) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(47))—

(I) does not include information or statements contained in any documents or materials filed with the Securities and Exchange Commission, or with Federal banking regulators, pursuant to section 12(i) of the Securities Exchange Act of 1934 (15 U.S.C. 781(I)); and

(II) with respect to the submittal of critical infrastructure information, does not include any disclosure or writing that when made accompanied the solicitation of an offer or a sale of securities; and

(ii) does not include information or statements submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings.

(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).

* * * * * * *

Subtitle C—Information Security

* * * * * * *

SEC. 226. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

(a) DEFINITIONS.—In this section—

(1) the term "cybersecurity risk" means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of information or information systems, including such related consequences caused by an act of terrorism;

(2) the term "incident" means an occurrence that—

(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system; or

(B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies;

(3) the term "information sharing and analysis organization" has the meaning given that term in section 212(5); **[**and**]**

(4) the term "information system" has the meaning given that term in section 3502(8) of title 44, United States Code**[**.**]***; and*

(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 discerning 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) CENTER.—There is in the Department a national cybersecurity and communications integration center (referred to in this section as the "Center") to carry out certain responsibilities of the Under Secretary appointed under section 103(a)(1)(H).

(c) FUNCTIONS.—The cybersecurity functions of the Center shall include—

(1) being ⟦a Federal civilian interface⟧ *the lead Federal civilian interface* for the multi-directional and cross-sector sharing of information related to ⟦cybersecurity risks,⟧ *cyber threat indicators, defensive measures, cybersecurity risks,* incidents, analysis, and warnings for Federal and non-Federal entities;

(2) providing shared situational awareness to enable real-time, integrated, and operational actions across the Federal

Government and non-Federal entities to address cybersecurity risks and incidents to Federal and non-Federal entities;

(3) coordinating the sharing of information related to [cybersecurity risks] *cyber threat indicators, defensive measures, cybersecurity risks,* and incidents across the Federal Government;

(4) facilitating cross-sector coordination to address cybersecurity risks and incidents, including cybersecurity risks and incidents that may be related or could have consequential impacts across multiple sectors;

(5)(A) conducting integration and analysis, including cross-sector integration and analysis, of [cybersecurity risks] *cyber threat indicators, defensive measures, cybersecurity risks,* and incidents; and

(B) sharing the analysis conducted under subparagraph (A) with Federal and non-Federal entities;

(6) upon request, providing timely technical assistance, risk management support, and incident response capabilities to Federal and non-Federal entities with respect to [cybersecurity risks] *cyber threat indicators, defensive measures, cybersecurity risks,* and incidents, which may include attribution, mitigation, and remediation; [and]

(7) providing information and recommendations on security and resilience measures to Federal and non-Federal entities, including information and recommendations to—

(A) facilitate information security; [and]

(B) strengthen information systems against cybersecurity risks and incidents[.]*; and*

(C) sharing cyber threat indicators and defensive measures;

(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 cybersecurity 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.

(d) COMPOSITION.—

(1) IN GENERAL.—The Center shall be composed of—

(A) appropriate representatives of Federal entities, such as—

(i) sector-specific agencies;

(ii) civilian and law enforcement agencies; and

(iii) elements of the intelligence community, as that term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4));

(B) appropriate representatives of non-Federal entities, such as—

(i) State [and local], *local, and tribal* governments;

(ii) information sharing and analysis organizations*, including information sharing and analysis centers*; [and]

(iii) owners and operators of critical information systems;

(iv) private entities.

(C) components within the Center that carry out cybersecurity and communications activities;

(D) a designated Federal official for operational coordination with and across each sector; [and]

(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

[(E)] *(J)* other appropriate representatives or entities, as determined by the Secretary.

(2) INCIDENTS.—In the event of an incident, during exigent circumstances the Secretary may grant a Federal or non-Federal entity immediate temporary access to the Center.

(e) PRINCIPLES.—In carrying out the functions under subsection (c), the Center shall ensure—

(1) to the extent practicable, that—

(A) timely, actionable, and relevant *cyber threat indicators, defensive measures, and* information related to cybersecurity risks, incidents, and analysis is shared;

(B) when appropriate, *cyber threat indicators, defensive measures, and* information related to cybersecurity risks, incidents, and analysis is integrated with other relevant information and tailored to the specific characteristics of a sector;

(C) activities are prioritized and conducted based on the level of risk;

(D) industry sector-specific, academic, and national laboratory expertise is sought and receives appropriate consideration;

(E) continuous, collaborative, and inclusive coordination occurs—

(i) across sectors; and

(ii) with—

(I) sector coordinating councils;

(II) information sharing and analysis organizations; and

(III) other appropriate non-Federal partners;

(F) as appropriate, the Center works to develop and use mechanisms for sharing information related to [cybersecurity risks] *cyber threat indicators, defensive measures, cybersecurity risks,* and incidents that are technology-neutral, interoperable, real-time, cost-effective, and resilient; [and]

(G) the Center works with other agencies to reduce unnecessarily duplicative sharing of information related to [cybersecurity risks] *cyber threat indicators, defensive measures, cybersecurity risks,* and incidents;

(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;

(2) that information related to [cybersecurity risks] *cyber threat indicators, defensive measures, cybersecurity risks,* and incidents is appropriately safeguarded against unauthorized access *or disclosure*; and

(3) that activities conducted by the Center comply with all policies, regulations, and laws that protect the privacy and civil liberties of United States persons*, 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)*.

(f) NO RIGHT OR BENEFIT.—

(1) IN GENERAL.—The provision of assistance or information to, and inclusion in the Center of, governmental or private entities under this section shall be at the sole and unreviewable discretion of the Under Secretary appointed under section 103(a)(1)(H).

(2) CERTAIN ASSISTANCE OR INFORMATION.—The provision of certain assistance or information to, or inclusion in the Center of, one governmental or private entity pursuant to this section shall not create a right or benefit, substantive or procedural, to similar assistance or information for any other governmental or private entity.

(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 Cooperative 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 Department, 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 consultation 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 report 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 provision 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. 227. CYBER INCIDENT RESPONSE [PLAN] *PLANS*.

[The Under Secretary appointed under section 103(a)(1)(H) shall**]** *(a) IN GENERAL.—The Under Secretary for Cybersecurity and Infrastructure Protection shall*, in coordination with appropriate Federal departments and agencies, State and local governments, sector coordinating councils, information sharing and analysis organizations (as defined in section 212(5)), owners and operators of critical infrastructure, and other appropriate entities and individuals, develop, regularly update, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks (as defined in section 226) to critical infrastructure.

(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.

* * * * * * *

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 stakeholders 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 stake-

holders in government, industry, academia, and the non-profit community in carrying out this section.

* * * * * * *

TITLE III—SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY

* * * * * * *

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 coordinate 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.

* * * * * * *

ADDITIONAL VIEWS

On behalf of Committee on Homeland Security Democrats, I submit the following additional views on H.R. 1731, the "National Cybersecurity Protection Advancement Act of 2015," as amended.

Improving cyber information sharing is a top legislative priority for Committee on Homeland Security Democrats for the 114th Congress. H.R. 1731 is the product of months of bipartisan stakeholder discussions with private sector stakeholders, including representatives from critical infrastructure sectors, technology companies, privacy organizations, as well as Federal stakeholders, most especially the Department of Homeland Security. Committee Democrats support efforts to bolster information sharing with the Department and agree with President Obama about the need for targeted liability protection to address addressing what some in industry have identified as a major barrier to sharing cyber threat information—the risk that sharing such information would expose companies to legal liability. Committee Democrats are disappointed that while the Majority worked collaboratively with us on the bulk of this legislation, when it came time to crafting liability protection language, Democrats were shut out. The liability protection provision that was negotiated between Chairman Michael McCaul and House Judiciary Committee Chairman Bob Goodlatte is unduly complicated and runs the risk of directly or inadvertently providing liability relief to entities that act negligently as lawsuits would only be allowed for "willful misconduct." It also may incentivize companies to not act on timely cyber threat information as it explicitly immunizes a non-Federal entity who "in good faith fails to act" on cyber information against lawsuits. This approach is counter to the fundamental goal of the Act—to provide companies with timely information to act and protect their networks and the information stored on them.

Although Committee Democrats are disappointed with the liability protection provision in H.R. 1731, Committee Democrats are pleased that our efforts to bolster the privacy provisions in the underlying bill were largely successful; however, it is worth noting that bipartisan discussions continue with privacy stakeholders about further refinements, as this measure moves to the Full House.

In general, we are pleased that H.R. 1731, as amended, limits the sharing and allowable uses for cyber threat information to "solely for cybersecurity purposes," requires participating non-Federal entities and the National Cybersecurity and Communications Integration Center (NCCIC) to remove unrelated information that identifies persons from cyber threat data (minimization), and builds in privacy protections and oversight at all levels of the NCCIC operation.

Committee Democrats are disappointed that amendments offered by Cybersecurity, Infrastructure Protection, and Security Technologies (CIPST) Subcommittee Ranking Member Cedric Richmond to improve the liability protection language were rejected at the Full Committee markup. They would have streamlined the language in key respects. Also rejected was an amendment that I offered to sunset this Act after five years to allow for the Committee to make adjustments to the law based on oversight findings.

Committee Democrats are pleased, however that twelve amendments offered by Committee Democrats were accepted. Two amendments that we would like to highlight in particular would seek to bolster the reach of this bill to Main Street America and every U.S. household.

The first was offered by CIPST Ranking Member Richmond. It directed DHS to bolster outreach to small and medium-size business, and to help ensure that Main Street businesses get the attention and assistance they need. Most small and medium-size businesses do not have the resources to focus on cyber threats but by requiring DHS to amplify its efforts with respect to small and medium-size businesses specifically regarding cyber security, we can help Main Street America participate, ensuring that information-sharing, on the larger scale, adds to the cyber security of a broad array of businesses all across our nation.

The second was offered by Oversight and Management Efficiency Subcommittee Ranking Member Bonnie Watson Coleman. It directs DHS to begin a concerted and sustained campaign to raise national awareness about cybersecurity. The campaign is to include public service announcements, widely advertised web sites, Apps, written collateral; social media; and other creative sources to help Americans understand that many simple measures will improve their cyber security protection posture. Such measures include simple steps like: improving password management; enabling firewall protection; installing anti-virus and anti-spam protection; installing software updates; "know your sender" and refrain from opening links and attachments from unknown and untrusted senders.

As we work to enhance information sharing about cyber threats, it is important to keep in mind that as much as 80 percent of exploitable vulnerabilities in cyberspace are a direct result of poor, or no cyber hygiene and software vulnerabilities. The American people must be made more aware about the basic fundamentals of cybersecurity.

Sincerely,

BENNIE G. THOMPSON,
Ranking Member.

○