[DISCUSSION DRAFT]

114TH CONGRESS
1ST SESSION

H. R. _____

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

IN THE HOUSE OF REPRESENTATIVES

Mr. MCCAUL introduced the following bill; which was referred to the Committee on _____

A BILL

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

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''National Cybersecurity Protection Advancement Act of 2015''.

SEC. 2. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

(a) DEFINITIONS.—

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

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

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

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

''(5) the term 'cyber threat indicator' means technical information—

''(A) that is necessary to describe or identify—

''(i) a method for probing or maintaining 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 or incident, including communications

that reasonably appear to be transmitted for the purpose of gathering technical information related to a cybersecurity risk or incident;

''(ii) a method for defeating a technical or security control for an information system that is primarily implemented and executed by people;

''(iii) a technical vulnerability;

''(iv) 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 inadvertently to enable the defeat of a technical or operational control;

''(v) a method for 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 cyber risk or incident; or

''(vi) any combination of clauses (i) through (v); and

''(B) from which reasonable efforts have been made to remove information that can be used to identify specific persons reasonably believed to be unrelated to the cybersecurity risk or incident;

''(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) the term 'defensive measure' means automated or manual actions taken by or on behalf of a Federal entity or non-Federal entity on an information system owned or operated by such Federal entity or non-Federal entity to modify or block data packets associated with electronic or wire communications, internet traffic, program code, or other system traffic transiting to or from or stored on such information system for the purpose of protecting such information system from a cybersecurity risk or incident, but such term does not include any automated or manual action designed or deployed in a manner that destroys, disables, or substantially harms an information system not owned or operated by—

"(A) the Federal entity or non-Federal entity owning or operating such an automated or manual action; or

"(B) another non-Federal entity or Federal entity that has provided consent to the first Federal entity or non-Federal entity for operation of such an automated or manual action in accordance with this section;

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

"(9) the term 'private entity' means an individual, a private or publicly traded company, a private or public utility (including a utility that is a unit of a State, local, or tribal government, or a political subdivision of a State government), an organization, or a corporation, including an officer, employee, or agent thereof;

"(10) 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 primary Federal civilian interface''; and

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

(B) in paragraph (2), by inserting ''share cyber threat indicators and defensive measures and'' before ''address'';

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

(D) in paragraph (4)—

(i) by inserting ''share cyber threat indicators and defensive measures and'' before ''address''; and

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

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

(F) in paragraph (6), by striking ''cybersecurity risks'' and inserting ''cyber threat indicators, defensive measures, cybersecurity risks,'';

(G) 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, defensive measures, and information related to cybersecurity risks and incidents;''; and

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

''(8) engage with international partners 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 the global cybersecurity ecosystem; and

''(9) sharing cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents with Federal and non-Federal entities.'';

(2) in subsection (d)—

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

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

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

''(E) a Multi-State Information Sharing and Analysis Center to collaborate with State and local governments;

''(F) a United States Computer Emergency Readiness Team to coordinate information related to cybersecurity risks and incidents, proactively manage cybersecurity risks and incidents to the United States, collaboratively respond to cybersecurity risks and incidents, provide technical assistance to information system owners and operators, and disseminate timely information related to cybersecurity risks and incidents;

''(G) the Industrial Control System Cyber Emergency Response Team to coordinate with industrial control systems owners and operators and share industrial control systems-related security incidents and mitigation measures;

''(H) National Coordinating Center for Communications to coordinate the protection,

response, and recovery of national security emergency communications; 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,''; and

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

(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), insert before the period at the end the following: ", including by working with the privacy officer appointed under section 222"; 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 shall develop a capability that supports and rapidly advances the development, adoption, and implementation of an automated mechanism for the timely sharing of cyber threat indicators and defensive measures to and from the Center.

"(2) BIANNUAL REPORT.—The Under Secretary for Cybersecurity and Infrastructure Protection shall submit to the appropriate congressional committees 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) VOLUNTARY INFORMATION SHARING PROCEDURES.—

"(1) 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, defensive measures, and information related to cybersecurity risks and incidents 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 and intentionally violated the terms of this subsection.

''(2) AGREEMENTS.—

''(A) CENTER MEMORANDUM OF UNDERSTANDING.—To enter into a voluntary information sharing relationship with the Center under this subsection, a consenting non-Federal entity shall enter into a memorandum of understanding with the Center that sets forth the general terms of the relationship, including all information sharing procedures set forth in any cooperative research and development agreements or appendices in effect as of March 15,

2015, and all information protections and liability exemptions specified in this subsection. A memorandum of understanding described in this subparagraph shall be finalized within 30 days of a request by a consenting non-Federal entity to enter into a voluntary information sharing relationship with the Center unless the Secretary, for national security purposes, declines to enter into such a relationship. Such memorandum of understanding shall be the only agreement required to enter into a formal information sharing relationship with the Center. Any information sharing agreement between the Center and a non-Federal entity in effect prior to the date of the enactment of this section is deemed in compliance with the requirements of this subsection.

''(B) OTHER AGREEMENTS.—Nothing in this subsection shall preclude the Department or the Center from entering into information sharing agreements other than a memorandum of understanding as set forth in subparagraph (A) with consenting non-Federal entities. All such other agreements shall include all informa-

tion protections and liability exemptions as set forth in this section.

''(3) INFORMATION SHARING 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, share cyber threat indicators, defensive measures, or information related to cybersecurity risks and incidents obtained on its own information system 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 cybersecurity risk indicator, defensive measure, or information related to cybersecurity risks and incidents from another Federal or non-Federal entity shall comply with otherwise lawful restrictions placed on the sharing or use of such cybersecurity risk indicator, defensive measure or information re-

lated to cybersecurity risks and incidents by the sharing Federal or non-Federal entity.

''(C) REMOVAL OF INFORMATION UNRELATED TO CYBERSECURITY RISKS OR INCIDENTS.—A non-Federal entity shall take reasonable efforts to minimize information that can be used to identify specific persons and is reasonably believed to be unrelated to a cybersecurity risk or incident, and to safeguard information that can be used to identify specific persons from unintended disclosure and 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.

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

"(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 the receipt, retention, use, and disclosure of cyber threat indicators, defensive measures, and information related to cybersecu-

rity risks and incidents associated with specific persons that is not necessary, for cybersecurity purposes, to protect an information system from cybersecurity risks and incidents 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 timely removal and destruction of obsolete or erroneous names and personal information that is unrelated to the cybersecurity risk or incident information shared in accordance with this section;

''(V) include requirements to safeguard cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents, 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, defensive measures, and information related to cybersecurity risks and incidents associated with specific persons to the greatest extent practicable;

"(VII) not delay or impede the flow of cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents necessary to defend against or mitigate cybersecurity risks and incidents; and

"(VIII) 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 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 appropriate congressional committees the policies and procedures governing the sharing of cyber threat indicators, defensive measures, and information related to cybersecurity 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 polices and procedures governing the sharing of cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents.

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

"(i) implement the policies and procedures governing the sharing of cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents established pursuant to clause (i) of subparagraph (A);

"(ii) annually prepare privacy impact assessments to ensure all relevant constitutional, legal, and privacy protections are being followed;

"(iii) promptly notify the Secretary and the appropriate congressional committees of any significant violations of such policies and procedures;

"(iv) annually submit to the appropriate congressional committees a report that contains an audit of the effectiveness of such policies and procedures;

"(v) promptly notify non-Federal entities that have shared cyber threat indicators, defensive measures, or information related to cybersecurity risks or incidents

that is known or determined to be in error or in contravention of the requirements of this section; and

''(vii) ensure there are appropriate sanctions in place for officers, employees, or agents of the Department who knowingly and 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, defensive measures, or information related to cybersecurity risks and incidents shared with the Center under this section, shall annually submit to the appropriate congressional committees 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, defensive measures, and information related to cybersecurity risks and incidents

that has been shared with Federal entities under this section.

''(ii) A review of 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) Appropriate metrics 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, defensive measures, and information related to cybersecurity risks and incidents shared with the Center under this section, shall annually 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, defensive measures, and information related to cybersecurity risks and incidents 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, defensive measures, or information related to cybersecurity risks or incidents through the Center or otherwise under this section—

''(i) may use, retain, or further disclose such cyber threat indicators, defensive measures, and information related to cybersecurity risks or incidents solely for cybersecurity purposes;

''(ii) shall take reasonable efforts to minimize information that can be used to identify specific persons and is reasonably believed to be unrelated to a cybersecurity risk or incident, and to safeguard information that can be used to identify specific persons from unintended disclosure and 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, defensive measures, and information related to cybersecurity risks and incidents that it discloses to other Federal entities or non-Federal entities;

''(iv) shall be deemed voluntarily shared;

''(v) shall implement and utilize a security control to protect against unauthorized access to or acquisition of such cyber threat indicators, defensive measures, or information related to cybersecurity risks or incidents; and

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

''(B) FEDERAL ENTITIES.—A Federal entity that receives cyber threat indicators, defensive measures, or information related to cybersecurity risks or incidents shared through the Center or otherwise under this section—

''(i) may use, retain, or further disclose such cyber threat indicators, defensive measures, and information related to

cybersecurity risks or incidents solely for cybersecurity purposes;

''(ii) shall take reasonable efforts to minimize information that can be used to identify specific persons and is reasonably believed to be unrelated to a cybersecurity risk or incident, and to safeguard information that can be used to identify specific persons from unintended disclosure and unauthorized access or acquisition;

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

''(iv) shall be deemed voluntarily shared;

''(v) shall implement and utilize a security control to protect against unauthorized access to or acquisition of such cyber threat indicators, defensive measures, or information related to cybersecurity risks or incidents;

''(vi) is 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;

''(vii) shall be considered proprietary information and may not be disclosed to an entity outside the Federal Government unless otherwise expressly authorized by the non-Federal entity sharing such information or anonymized to protect source information.

''(viii) may not be used by the Federal Government for regulatory purposes;

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

''(x) shall be considered the commercial, financial, and proprietary information of such non-Federal entity when so designated by such non-Federal entity; and

''(xi) 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, TRIBAL, OR LOCAL GOVERNMENT.—Cyber threat indicators, defensive measures, or information related to cybersecurity risks or incidents shared with a State, tribal, or local government by the Center or otherwise under this section—

''(i) may use, retain, or further disclose such cyber threat indicators, defensive measures, and information related to cybersecurity risks or incidents solely for cybersecurity purposes;

''(ii) shall take reasonable efforts to minimize information that can be used to identify specific persons and is reasonably believed to be unrelated to a cybersecurity risk or incident, and to safeguard information that can be used to identify specific persons from unintended disclosure and 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 indi-

cators, defensive measures, and information related to cybersecurity risks and incidents that it discloses to other Federal entities or non-Federal entities;

''(iv) shall be deemed voluntarily shared;

''(v) shall implement and utilize a security control to protect against unauthorized access to or acquisition of such cyber threat indicators, defensive measures, or information related to cybersecurity risks or incidents;

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

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

''(8) LIABILITY EXEMPTIONS.—

''(A) IN GENERAL.—A non-Federal entity, not including a State, local, or tribal government, that, for cybersecurity purposes, in accordance with paragraphs (3) and (4), shares

cyber threat indicators, defensive measures, or information related to cybersecurity risks or incidents or conducts network awareness on an information system shall not be liable in any civil or criminal action brought under this subsection unless such non-Federal entity engaged in willful misconduct or gross negligence with respect to such sharing or conduct and such gross negligence or willful misconduct proximately caused injury.

''(B) GROSS NEGLIGENCE.—The term 'gross negligence' shall, for purposes of this subsection, mean an act or omission—

''(i) which when viewed objectively from the standpoint of the non-Federal entity at issue at the time of the occurrence of such act or omission involves an extreme degree of risk, considering the substantial probability and magnitude of the potential harm to others; and

''(ii) of which such non-Federal entity has actual, subjective awareness of the risk involved, but nevertheless proceeds with conscious, flagrant indifference to the rights or safety of others.

"(C) WILLFUL MISCONDUCT.—The term 'willful misconduct' shall, for purposes of this subsection, mean 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 resulting from taking such act or omission will outweigh the benefit.

"(D) RULE OF CONSTRUCTION.—Notwithstanding any other provision of law, a non-Federal entity shall not have engaged in gross negligence or willful misconduct as a matter of law if such non-Federal entity acted in accordance with this section or applicable directions, guidelines, or recommendations by the Secretary regarding the administration or use of an information system.

"(E) PROOF OF GROSS NEGLIGENCE OR WILLFUL MISCONDUCT.—In an action under subparagraph (A), the plaintiff shall have the

burden of proving by clear and convincing evidence gross negligence or willful misconduct by each non-Federal entity sued, and that such gross negligence or willful misconduct proximately caused such plaintiff's injury. Punitive damages intended to punish or deter, exemplary damages, or other damages not intended to compensate a plaintiff for actual losses may be awarded in such an action only if a plaintiff proves that a non-Federal entity engaged in willful misconduct.

''(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 (7)(B) on the use and protection of voluntarily shared cyber threat indicators, defensive measures, or information related to cybersecurity risks or incidents, 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) the costs of the action, together with reasonable attorney fees as determined by the court.

"(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 7(B) 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 7(B).

"(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, defensive measure, or information related to cybersecurity risks and incidents, 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 cybersecurity risk indicator, defensive measure, or information related to a cybersecurity risk or incident 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, boycotting, 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, 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, defensive measures, and information related to cybersecurity risks and incidents with a non-Federal entity on such non-Federal entity's provision of cyber threat indicators to a Federal entity; or

''(iii) condition the award of any Federal grant, contract, or purchase on the sharing of cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents 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 participate 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.''.

SEC. 4. PROTECTION OF FEDERAL CIVILIAN INFORMATION SYSTEMS.

(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 section:

''SEC. 230. PROTECTION OF FEDERAL INFORMATION SYSTEMS.

''(a) IN GENERAL.—The Secretary shall—

''(1) administer Federal Government-wide efforts to develop and provide adequate, risk-based, cost-effective, and technology neutral information security capabilities;

''(2) establish and sustain continuous diagnostics systems for Federal civilian information systems to aggregate data and identify and prioritize the mitigation of cybersecurity risks and incidents in such systems for cybersecurity purposes;

''(3) develop, acquire, and operate an integrated and consolidated system of intrusion detection, analytics, intrusion prevention, and other information sharing and protective capabilities to defend Federal

civilian information systems from cybersecurity risks and incidents;

''(4) develop and conduct targeted risk assessments and operational evaluations of Federal civilian information systems, in consultation with Federal entities and non-Federal entities that own and operate Federal civilian information systems, including threat, vulnerability, and impact assessments and penetration testing;

''(5) develop and provide technical assistance and cyber incident response capabilities to secure and ensure the resilience of Federal civilian information systems;

''(6) develop reporting requirements, consistent with relevant law, to ensure the National Cybersecurity and Communications Integration Center established pursuant to the second section 226 receives all actionable information related to cybersecurity risks and incidents; and

''(7) develop training requirements regarding privacy, civil rights, civil liberties, and information oversight for information security employees who operate Federal civilian information systems.

''(b) USE OF CERTAIN COMMUNICATIONS.—

''(1) IN GENERAL.—The Secretary may enter into contracts or other agreements, or otherwise request and obtain, in accordance with applicable law, the assistance of private entities that provide electronic communication services, remote computing services, or cybersecurity services to acquire, intercept, retain, use, and disclose communications and other system traffic, deploy defensive measures (as such term is defined in the second section 226 (relating to the National Cybersecurity and Communications Integration Center)), or otherwise operate protective capabilities in accordance with paragraphs (2), (3), (4), and (5) of subsection (a). No cause of action shall exist against private entities for assistance provided to the Secretary in accordance with this subsection.

''(2) RULE OF CONSTRUCTION.—Nothing in paragraph (1) may be construed to—

''(A) require or compel any private entity to enter in a contract or agreement described in such paragraph; or

''(B) authorize the Secretary to take any action with respect to any communications or system traffic transiting or residing on any in-

formation system other than a Federal civilian information system.''.

SEC. 5. 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''; 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. 6. 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. 7. STREAMLINING OF DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY AND INFRASTRUCTURE PROTECTION ORGANIZATION.

(a) CYBERSECURITY AND INFRASTRUCTURE PROTECTION DIRECTORATE.—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 Directorate''. 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 Directorate of the Department.

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

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

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

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

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

''(K) A Deputy Under Secretary for Cybersecurity.

''(L) A Deputy Under Secretary for Infrastructure Protection.''.

(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.—To improve the operational capability and effectiveness in carrying out the cybersecurity mission of the Department of Homeland Security, 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 Government Affairs of the Senate a report on the feasibility of making the Cybersecurity and Communications Office of the Department an operational component of the Department.

SEC. 8. CONFORMING AMENDMENTS.

Subsection (b) of section 552 of title 5, United States Code, is amended—

(1) in paragraph (8), by striking ''or'' at the end;

(2) in paragraph (9), by striking the period at the end and inserting ''; or''; and

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

''(10) information shared with or provided to the Department of Homeland Security pursuant to 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).''.