DIVISION N—CYBERSECURITY ACT OF 2015

SEC. 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This division may be cited as the ''Cybersecurity Act of 2015''.

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

TITLE I—CYBERSECURITY INFORMATION SHARING

SEC. 101. SHORT TITLE.

This title may be cited as the ''Cybersecurity Information Sharing Act of 2015''.

SEC. 102. DEFINITIONS.

In this title:

(1) AGENCY.—The term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code.

(2) ANTITRUST LAWS.—The term ''antitrust laws''—

(A) has the meaning given the term in the first section of the Clayton Act (15 U.S.C. 12);

(B) includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that section 5 of that Act applies to unfair methods of competition; and

(C) includes any State antitrust law, but only to the extent that such law is consistent with the law referred to in subparagraph (A) or the law referred to in subparagraph (B).

(3) APPROPRIATE FEDERAL ENTITIES.—The term ''appropriate Federal entities'' means the following:

(A) The Department of Commerce.

(B) The Department of Defense.

(C) The Department of Energy.

(D) The Department of Homeland Security.

(E) The Department of Justice.

(F) The Department of the Treasury.

(G) The Office of the Director of National Intelligence.

(4) CYBERSECURITY PURPOSE.—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 threat or security vulnerability.

(5) CYBERSECURITY THREAT.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term ''cybersecurity threat'' means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

(B) EXCLUSION.—The term ''cybersecurity threat'' does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

(6) CYBER THREAT INDICATOR.—The term ''cyber threat indicator'' means information that is necessary to describe or identify—

(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gath-

ering technical information related to a cybersecurity threat or security vulnerability;

(B) a method of defeating a security control or exploitation of a security vulnerability;

(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security 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 unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

(E) malicious cyber command and control;

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

(G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

(H) any combination thereof.

(7) DEFENSIVE MEASURE.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term ''defensive meas-

ure'' 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 threat or security vulnerability.

(B) EXCLUSION.—The term ''defensive measure'' does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by—

(i) the private entity operating the measure; or

(ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

(8) FEDERAL ENTITY.—The term ''Federal entity'' means a department or agency of the United States or any component of such department or agency.

(9) INFORMATION SYSTEM.—The term ''information system''—

(A) has the meaning given the term in section 3502 of title 44, United States Code; and

(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

(10) LOCAL GOVERNMENT.—The term ''local government'' means any borough, city, county, parish, town, township, village, or other political subdivision of a State.

(11) MALICIOUS CYBER COMMAND AND CONTROL.—The term ''malicious cyber command and control'' means 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.

(12) MALICIOUS RECONNAISSANCE.—The term ''malicious reconnaissance'' means a method for actively probing or passively monitoring an information system for the purpose of discerning security vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(13) MONITOR.—The term ''monitor'' means to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system.

(14) NON-FEDERAL ENTITY.—

(A) IN GENERAL.—Except as otherwise provided in this paragraph, the term ''non-Federal entity'' means any private entity, non-Federal government agency or department, or State, tribal, or local government (including a political subdivision, department, or component thereof).

(B) INCLUSIONS.—The term ''non-Federal entity'' includes a government agency or department of the District of Columbia, the Commonwealth of Puerto Rico, the United States Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States.

(C) EXCLUSION.—The term ''non-Federal entity'' does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(15) PRIVATE ENTITY.—

(A) IN GENERAL.—Except as otherwise provided in this paragraph, the term ''private entity'' means any person or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity, including an officer, employee, or agent thereof.

(B) INCLUSION.—The term ''private entity'' includes a State, tribal, or local government performing utility services, such as electric, natural gas, or water services.

(C) EXCLUSION.—The term ''private entity'' does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(16) SECURITY CONTROL.—The term ''security control'' means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

(17) SECURITY VULNERABILITY.—The term ''security vulnerability'' means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

(18) TRIBAL.—The term ''tribal'' has the meaning given the term ''Indian tribe'' in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

SEC. 103. SHARING OF INFORMATION BY THE FEDERAL GOVERNMENT.

(a) IN GENERAL.—Consistent with the protection of classified information, intelligence sources and methods, and privacy and civil liberties, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation with the heads of the appropriate Federal entities, shall jointly develop and issue procedures to facilitate and promote—

(1) the timely sharing of classified cyber threat indicators and defensive measures in the possession of the Federal Government with representatives of relevant Federal entities and non-Federal entities that have appropriate security clearances;

(2) the timely sharing with relevant Federal entities and non-Federal entities of cyber threat indicators, defensive measures, and information relating to cybersecurity threats or authorized uses under this title, in the possession of the Federal Government

that may be declassified and shared at an unclassified level;

(3) the timely sharing with relevant Federal entities and non-Federal entities, or the public if appropriate, of unclassified, including controlled unclassified, cyber threat indicators and defensive measures in the possession of the Federal Government;

(4) the timely sharing with Federal entities and non-Federal entities, if appropriate, of information relating to cybersecurity threats or authorized uses under this title, in the possession of the Federal Government about cybersecurity threats to such entities to prevent or mitigate adverse effects from such cybersecurity threats; and

(5) the periodic sharing, through publication and targeted outreach, of cybersecurity best practices that are developed based on ongoing analyses of cyber threat indicators, defensive measures, and information relating to cybersecurity threats or authorized uses under this title, in the possession of the Federal Government, with attention to accessibility and implementation challenges faced by small business concerns (as defined in section 3 of the Small Business Act (15 U.S.C. 632)).

(b) DEVELOPMENT OF PROCEDURES.—

(1) IN GENERAL.—The procedures developed under subsection (a) shall—

(A) ensure the Federal Government has and maintains the capability to share cyber threat indicators and defensive measures in real time consistent with the protection of classified information;

(B) incorporate, to the greatest extent practicable, existing processes and existing roles and responsibilities of Federal entities and non-Federal entities for information sharing by the Federal Government, including sector specific information sharing and analysis centers;

(C) include procedures for notifying, in a timely manner, Federal entities and non-Federal entities that have received a cyber threat indicator or defensive measure from a Federal entity under this title that is known or determined to be in error or in contravention of the requirements of this title or another provision of Federal law or policy of such error or contravention;

(D) include requirements for Federal entities sharing cyber threat indicators or defensive

measures to implement and utilize security controls to protect against unauthorized access to or acquisition of such cyber threat indicators or defensive measures;

(E) include procedures that require a Federal entity, prior to the sharing of a cyber threat indicator—

(i) to review such cyber threat indicator to assess whether such cyber threat indicator contains any information not directly related to a cybersecurity threat that such Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual and remove such information; or

(ii) to implement and utilize a technical capability configured to remove any information not directly related to a cybersecurity threat that the Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual; and

(F) include procedures for notifying, in a timely manner, any United States person whose personal information is known or determined to have been shared by a Federal entity in violation of this title.

(2) CONSULTATION.—In developing the procedures required under this section, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General shall consult with appropriate Federal entities, including the Small Business Administration and the National Laboratories (as defined in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801)), to ensure that effective protocols are implemented that will facilitate and promote the sharing of cyber threat indicators by the Federal Government in a timely manner.

(c) SUBMITTAL TO CONGRESS.—Not later than 60 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the heads of the appropriate Federal entities, shall submit to Congress the procedures required by subsection (a).

SEC. 104. AUTHORIZATIONS FOR PREVENTING, DETECTING, ANALYZING, AND MITIGATING CYBERSECURITY THREATS.

(a) AUTHORIZATION FOR MONITORING.—

(1) IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, monitor—

(A) an information system of such private entity;

(B) an information system of another non-Federal entity, upon the authorization and written consent of such other entity;

(C) an information system of a Federal entity, upon the authorization and written consent of an authorized representative of the Federal entity; and

(D) information that is stored on, processed by, or transiting an information system monitored by the private entity under this paragraph.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed—

(A) to authorize the monitoring of an information system, or the use of any information obtained through such monitoring, other than as provided in this title; or

(B) to limit otherwise lawful activity.

(b) AUTHORIZATION FOR OPERATION OF DEFENSIVE MEASURES.—

(1) IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, operate a defensive measure that is applied to—

(A) an information system of such private entity in order to protect the rights or property of the private entity;

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

(C) 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 the Federal Government.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed—

(A) to authorize the use of a defensive measure other than as provided in this subsection; or

(B) to limit otherwise lawful activity.

(c) AUTHORIZATION FOR SHARING OR RECEIVING CYBER THREAT INDICATORS OR DEFENSIVE MEASURES.—

(1) IN GENERAL.—Except as provided in paragraph (2) and notwithstanding any other provision of law, a non-Federal entity may, for a cybersecurity purpose and consistent with the protection of classified information, share with, or receive from, any other non-Federal entity or the Federal Government a cyber threat indicator or defensive measure.

(2) LAWFUL RESTRICTION.—A non-Federal entity receiving a cyber threat indicator or defensive measure from another non-Federal entity or a 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 non-Federal entity or Federal entity.

(3) CONSTRUCTION.—Nothing in this subsection shall be construed—

(A) to authorize the sharing or receiving of a cyber threat indicator or defensive measure other than as provided in this subsection; or

(B) to limit otherwise lawful activity.

(d) PROTECTION AND USE OF INFORMATION.—