

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 450b of title 25.

(Pub. L. 114–113, div. N, title I, §102, Dec. 18, 2015, 129 Stat. 2936.)

SHORT TITLE

Pub. L. 114–113, div. N, §1(a), Dec. 18, 2015, 129 Stat. 2935, provided that: “This division [enacting this chapter and sections 149 and 151 of this title, amending sections 131, 148, 149, and 150 of this title, section 1029 of Title 18, Crimes and Criminal Procedure, and sections 3553 and 3554 of Title 44, Public Printing and Documents, enacting provisions set out as notes under this section and sections 101, 131, and 151 of this title and section 301 of Title 5, Government Organization and Employees] may be cited as the ‘Cybersecurity Act of 2015.’”

Pub. L. 114–113, div. N, title I, §101, Dec. 18, 2015, 129 Stat. 2936, provided that: “This title [enacting this subchapter] may be cited as the ‘Cybersecurity Information Sharing Act of 2015.’”

Pub. L. 114–113, div. N, title II, §221, Dec. 18, 2015, 129 Stat. 2963, provided that: “This subtitle [subtitle B (§§221–229) of title II of div. N of Pub. L. 114–113, enacting subchapter II of this chapter and sections 149 and 151 of this title, amending sections 148, 149, and 150 of this title and sections 3553 and 3554 of Title 44, Public Printing and Documents, and enacting provisions set out as a note under section 151 of this title] may be cited as the ‘Federal Cybersecurity Enhancement Act of 2015.’”

**§ 1502. 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 subchapter, 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 subchapter, 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 subchapter, in the possession of the Federal Government, with attention to accessibility and implementation challenges faced by small business concerns (as defined in section 632 of title 15).

**(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 subchapter that is known or determined to be in error or in contravention of the requirements of this subchapter 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 individ-

ual 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 subchapter.

**(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 15801 of title 42), 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 December 18, 2015, 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).

(Pub. L. 114–113, div. N, title I, § 103, Dec. 18, 2015, 129 Stat. 2939.)

**§ 1503. 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 subchapter; 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**

**(1) Security of information**

A non-Federal entity monitoring an information system, operating a defensive measure, or providing or receiving a cyber threat indicator or defensive measure under this section shall implement and utilize a security control to protect against unauthorized access to or acquisition of such cyber threat indicator or defensive measure.

**(2) Removal of certain personal information**

A non-Federal entity sharing a cyber threat indicator pursuant to this subchapter shall, prior to such sharing—

(A) review such cyber threat indicator to assess whether such cyber threat indicator contains any information not directly related to a cybersecurity threat that the non-Federal entity knows at the time of sharing to be personal information of a specific indi-