

(Pub. L. 114–113, div. N, title I, § 107, Dec. 18, 2015, 129 Stat. 2951.)

**§ 1507. Construction and preemption**

**(a) Otherwise lawful disclosures**

Nothing in this subchapter shall be construed—

(1) 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 entity to any other non-Federal entity or the Federal Government under this subchapter; or

(2) to limit or prohibit otherwise lawful use of such disclosures by any Federal entity, even when such otherwise lawful disclosures duplicate or replicate disclosures made under this subchapter.

**(b) Whistle blower protections**

Nothing in this subchapter shall be construed to prohibit or limit the disclosure of information protected under section 2302(b)(8) of title 5 (governing disclosures of illegality, waste, fraud, abuse, or public health or safety threats), section 7211 of title 5 (governing disclosures to Congress), section 1034 of title 10 (governing disclosure to Congress by members of the military), section 3234 of title 50 (governing disclosure by employees of elements of the intelligence community), or any similar provision of Federal or State law.

**(c) Protection of sources and methods**

Nothing in this subchapter shall be construed—

(1) as creating any immunity against, or otherwise affecting, any action brought by the Federal Government, or any agency or department thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, or use of classified information;

(2) to affect the conduct of authorized law enforcement or intelligence activities; or

(3) to modify the authority of a department or agency of the Federal Government to protect classified information and sources and methods and the national security of the United States.

**(d) Relationship to other laws**

Nothing in this subchapter shall be construed to affect any requirement under any other provision of law for a non-Federal entity to provide information to the Federal Government.

**(e) Prohibited conduct**

Nothing in this subchapter shall 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.

**(f) Information sharing relationships**

Nothing in this subchapter shall be construed—

(1) to limit or modify an existing information sharing relationship;

(2) to prohibit a new information sharing relationship;

(3) to require a new information sharing relationship between any non-Federal entity and a Federal entity or another non-Federal entity; or

(4) to require the use of the capability and process within the Department of Homeland Security developed under section 1504(c) of this title.

**(g) Preservation of contractual obligations and rights**

Nothing in this subchapter shall be construed—

(1) to 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

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

**(h) Anti-tasking restriction**

Nothing in this subchapter shall be construed to permit a Federal entity—

(1) to require a non-Federal entity to provide information to a Federal entity or another non-Federal entity;

(2) to condition the sharing of cyber threat indicators with a non-Federal entity on such entity's provision of cyber threat indicators to a Federal entity or another non-Federal entity; or

(3) to condition the award of any Federal grant, contract, or purchase on the provision of a cyber threat indicator to a Federal entity or another non-Federal entity.

**(i) No liability for non-participation**

Nothing in this subchapter shall be construed to subject any entity to liability for choosing not to engage in the voluntary activities authorized in this subchapter.

**(j) Use and retention of information**

Nothing in this subchapter shall 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 subchapter for any use other than permitted in this subchapter.

**(k) Federal preemption**

**(1) In general**

This subchapter 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 subchapter.

**(2) State law enforcement**

Nothing in this subchapter shall be construed to supersede any statute or other provision of law of a State or political subdivision of a State concerning the use of authorized law enforcement practices and procedures.

**(l) Regulatory authority**

Nothing in this subchapter shall be construed—

(1) to authorize the promulgation of any regulations not specifically authorized to be issued under this subchapter;

(2) to establish or limit any regulatory authority not specifically established or limited under this subchapter; or

(3) to authorize regulatory actions that would duplicate or conflict with regulatory requirements, mandatory standards, or related processes under another provision of Federal law.

**(m) Authority of Secretary of Defense to respond to malicious cyber activity carried out by foreign powers**

Nothing in this subchapter shall be construed to limit the authority of the Secretary of Defense under section 394 of title 10.

**(n) Criminal prosecution**

Nothing in this subchapter shall be construed to prevent the disclosure of a cyber threat indicator or defensive measure shared under this subchapter in a case of criminal prosecution, when an applicable provision of Federal, State, tribal, or local law requires disclosure in such case.

(Pub. L. 114–113, div. N, title I, § 108, Dec. 18, 2015, 129 Stat. 2953; Pub. L. 115–232, div. A, title XVI, § 1631(b), Aug. 13, 2018, 132 Stat. 2123.)

**Editorial Notes**

AMENDMENTS

2018—Subsec. (m). Pub. L. 115–232 substituted “section 394” for “section 130g”.

**§ 1508. Report on cybersecurity threats**

**(a) Report required**

Not later than 180 days after December 18, 2015, the Director of National Intelligence, in coordination with the heads of other appropriate elements of the intelligence community, shall submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives a report on cybersecurity threats, including cyber attacks, theft, and data breaches.

**(b) Contents**

The report required by subsection (a) shall include the following:

(1) An assessment of the current intelligence sharing and cooperation relationships of the United States with other countries regarding cybersecurity threats, including cyber attacks, theft, and data breaches, directed against the United States and which threaten the United States national security interests and economy and intellectual property, specifically identifying the relative utility of such relationships, which elements of the intelligence community participate in such relationships, and whether and how such relationships could be improved.

(2) A list and an assessment of the countries and nonstate actors that are the primary threats of carrying out a cybersecurity threat, including a cyber attack, theft, or data breach, against the United States and which threaten the United States national security, economy, and intellectual property.

(3) A description of the extent to which the capabilities of the United States Government

to respond to or prevent cybersecurity threats, including cyber attacks, theft, or data breaches, directed against the United States private sector are degraded by a delay in the prompt notification by private entities of such threats or cyber attacks, theft, and data breaches.

(4) An assessment of additional technologies or capabilities that would enhance the ability of the United States to prevent and to respond to cybersecurity threats, including cyber attacks, theft, and data breaches.

(5) An assessment of any technologies or practices utilized by the private sector that could be rapidly fielded to assist the intelligence community in preventing and responding to cybersecurity threats.

**(c) Form of report**

The report required by subsection (a) shall be made available in classified and unclassified forms.

**(d) Intelligence community defined**

In this section, the term “intelligence community” has the meaning given that term in section 3003 of title 50.

(Pub. L. 114–113, div. N, title I, § 109, Dec. 18, 2015, 129 Stat. 2955.)

**§ 1509. Exception to limitation on authority of Secretary of Defense to disseminate certain information**

Notwithstanding subsection (c)(3) of section 393 of title 10, the Secretary of Defense may authorize the sharing of cyber threat indicators and defensive measures pursuant to the policies, procedures, and guidelines developed or issued under this subchapter.

(Pub. L. 114–113, div. N, title I, § 110, Dec. 18, 2015, 129 Stat. 2956.)

**§ 1510. Effective period**

**(a) In general**

Except as provided in subsection (b), this subchapter and the amendments made by this subchapter shall be effective during the period beginning on December 18, 2015 and ending on September 30, 2025.

**(b) Exception**

With respect to any action authorized by this subchapter or information obtained pursuant to an action authorized by this subchapter, which occurred before the date on which the provisions referred to in subsection (a) cease to have effect, the provisions of this subchapter shall continue in effect.

(Pub. L. 114–113, div. N, title I, § 111, Dec. 18, 2015, 129 Stat. 2956.)

**Editorial Notes**

REFERENCES IN TEXT

The amendments made by this subchapter, referred to in subsec. (a), was in the original “the amendments made by this title”, meaning title I of div. N of Pub. L. 114–113, which is classified generally to this subchapter.