(2) Contents

Each report submitted under paragraph (1) shall include, for the period covered by the report, the following:

(A) An assessment of the sufficiency of the policies, procedures, and guidelines relating to the sharing of cyber threat indicators within the Federal Government, including those policies, procedures, and guidelines relating to the removal of information not directly related to a cybersecurity threat that is personal information of a specific individual or information that identifies a specific individual.

(B) An assessment of whether cyber threat indicators or defensive measures have been properly classified and an accounting of the number of security clearances authorized by the Federal Government for the purpose of sharing cyber threat indicators or defensive measures with the private sector.

(C) A review of the actions taken by the Federal Government based on cyber threat indicators or defensive measures shared with the Federal Government under this subchapter, including a review of the following:

(i) The appropriateness of subsequent uses and disseminations of cyber threat indicators or defensive measures.

(ii) Whether cyber threat indicators or defensive measures were shared in a timely and adequate manner with appropriate entities, or, if appropriate, were made publicly available.

(D) An assessment of the cyber threat indicators or defensive measures shared with the appropriate Federal entities under this subchapter, including the following:

(i) The number of cyber threat indicators or defensive measures shared through the capability and process developed under section 1504(c) of this title.

(ii) An assessment of any information not directly related to a cybersecurity threat that is personal information of a specific individual or information identifying a specific individual and was shared by a non-Federal government[1] entity with the Federal government[1] in contravention of this subchapter, or was shared within the Federal Government in contravention of the guidelines required by this subchapter, including a description of any significant violation of this subchapter.

(iii) The number of times, according to the Attorney General, that information shared under this subchapter was used by a Federal entity to prosecute an offense listed in section 1504(d)(5)(A) of this title.

(iv) A quantitative and qualitative assessment of the effect of the sharing of cyber threat indicators or defensive measures with the Federal Government on privacy and civil liberties of specific individuals, including the number of notices that were issued with respect to a failure to remove information not directly related to a cybersecurity threat that was personal information of a specific individual or information that identified a specific individual in accordance with the procedures required by section 1504(b)(3)(E) of this title.

(v) The adequacy of any steps taken by the Federal Government to reduce any adverse effect from activities carried out under this subchapter on the privacy and civil liberties of United States persons.

(E) An assessment of the sharing of cyber threat indicators or defensive measures among Federal entities to identify inappropriate barriers to sharing information.

(3) Recommendations

Each report submitted under this subsection may include such recommendations as the inspectors general may have for improvements or modifications to the authorities and processes under this subchapter.

(c) Independent report on removal of personal information

Not later than 3 years after December 18, 2015, the Comptroller General of the United States shall submit to Congress a report on the actions taken by the Federal Government to remove personal information from cyber threat indicators or defensive measures pursuant to this subchapter. Such report shall include an assessment of the sufficiency of the policies, procedures, and guidelines established under this subchapter in addressing concerns relating to privacy and civil liberties.

(d) Form of reports

Each report required under this section shall be submitted in an unclassified form, but may include a classified annex.

(e) Public availability of reports

The unclassified portions of the reports required under this section shall be made available to the public.

(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 disclo-

[1] So in original. Probably should be capitalized.

sure 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.)

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.)

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.

SUBCHAPTER II—FEDERAL CYBERSECURITY ENHANCEMENT

§ 1521. Definitions

In this subchapter:

(1) Agency

The term ''agency'' has the meaning given the term in section 3502 of title 44.

(2) Agency information system

The term ''agency information system'' has the meaning given the term in section 660 of this title.

(3) Appropriate congressional committees

The term ''appropriate congressional committees'' means—

(A) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) the Committee on Homeland Security of the House of Representatives.

(4) Cybersecurity risk; information system

The terms ''cybersecurity risk'' and ''information system'' have the meanings given those terms in section 659 of this title.

(5) Director

The term ''Director'' means the Director of the Office of Management and Budget.

(6) Intelligence community

The term ''intelligence community'' has the meaning given the term in section 3003(4) of title 50.