(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 130g 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.)

§ 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 149 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 148 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.

(7) National security system

The term ''national security system'' has the meaning given the term in section 11103 of title 40.

(8) Secretary

The term ''Secretary'' means the Secretary of Homeland Security.

(Pub. L. 114–113, div. N, title II, § 222, Dec. 18, 2015, 129 Stat. 2963.)

REFERENCES IN TEXT

This subchapter, referred to in text, was in the original ''this subtitle'', meaning subtitle B (§§ 221–229) of title II of div. N of Pub. L. 114–113, which is classified principally to this subchapter. For complete classification of subtitle B to the Code, see Tables.

§ 1522. Advanced internal defenses

(a) Advanced network security tools

(1) In general

The Secretary shall include, in the efforts of the Department to continuously diagnose and mitigate cybersecurity risks, advanced network security tools to improve visibility of network activity, including through the use of commercial and free or open source tools, and to detect and mitigate intrusions and anomalous activity.

(2) Development of plan

The Director shall develop and the Secretary shall implement a plan to ensure that each agency utilizes advanced network security tools, including those described in paragraph (1), to detect and mitigate intrusions and anomalous activity.

(b) Prioritizing advanced security tools

The Director and the Secretary, in consultation with appropriate agencies, shall—

(1) review and update Government-wide policies and programs to ensure appropriate prioritization and use of network security monitoring tools within agency networks; and

(2) brief appropriate congressional committees on such prioritization and use.

(c) Improved metrics

The Secretary, in collaboration with the Director, shall review and update the metrics used to measure security under section 3554 of title 44 to include measures of intrusion and incident detection and response times.

(d) Transparency and accountability

The Director, in consultation with the Secretary, shall increase transparency to the public on agency cybersecurity posture, including by increasing the number of metrics available on Federal Government performance websites and, to the greatest extent practicable, displaying metrics for department components, small agencies, and micro-agencies.

(e) Omitted

(f) Exception

The requirements under this section shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.