

§ 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.