6 USCS § 1508

Current through Public Law 118-62, approved May 13, 2024.

United States Code Service > TITLE 6. DOMESTIC SECURITY (§§ 101 — 1534) > CHAPTER 6. CYBERSECURITY (§§ 1500 — 1534) > CYBERSECURITY INFORMATION SHARING (§§ 1500 — 1510)

§ 1508. Report on cybersecurity threats

(a) Report required. Not later than 180 days after the date of the enactment of this Act [enacted Dec. 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 3 of the National Security Act of 1947 (50 U.S.C. 3003).

History

HISTORY:

Dec. 18, 2015, P. L. 114-113, Div N, Title I, § 109, 129 Stat. 2955.

End of Document