rectorate shall submit a report regarding the availability of, and benefits (including cost savings and security) of using, cybersecurity personnel and facilities outside of the National Capital Region (as defined in section 2674 of title 10) to serve the Federal and national need to—

(1) the Subcommittee on Homeland Security of the Committee on Appropriations and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(2) the Subcommittee on Homeland Security of the Committee on Appropriations and the Committee on Homeland Security of the House of Representatives.

(Pub. L. 107–296, title II, § 226, as added Pub. L. 113–277, § 3(a), Dec. 18, 2014, 128 Stat. 3005.)

CODIFICATION

Another section 226 of Pub. L. 107–296 is classified to section 148 of this title.

### § 148. National cybersecurity and communications integration center

**(a) Definitions**

In this section—

(1) the term ''cybersecurity risk'' means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of information or information systems, including such related consequences caused by an act of terrorism;

(2) the term ''incident'' means an occurrence that—

(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system; or

(B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies;

(3) the term ''information sharing and analysis organization'' has the meaning given that term in section 131(5) of this title; and

(4) the term ''information system'' has the meaning given that term in section 3502(8) of title 44.

**(b) Center**

There is in the Department a national cybersecurity and communications integration center (referred to in this section as the ''Center'') to carry out certain responsibilities of the Under Secretary appointed under section 113(a)(1)(H) of this title.

**(c) Functions**

The cybersecurity functions of the Center shall include—

(1) being a Federal civilian interface for the multi-directional and cross-sector sharing of information related to cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities;

(2) providing shared situational awareness to enable real-time, integrated, and operational actions across the Federal Government and non-Federal entities to address cybersecurity risks and incidents to Federal and non-Federal entities;

(3) coordinating the sharing of information related to cybersecurity risks and incidents across the Federal Government;

(4) facilitating cross-sector coordination to address cybersecurity risks and incidents, including cybersecurity risks and incidents that may be related or could have consequential impacts across multiple sectors;

(5)(A) conducting integration and analysis, including cross-sector integration and analysis, of cybersecurity risks and incidents; and

(B) sharing the analysis conducted under subparagraph (A) with Federal and non-Federal entities;

(6) upon request, providing timely technical assistance, risk management support, and incident response capabilities to Federal and non-Federal entities with respect to cybersecurity risks and incidents, which may include attribution, mitigation, and remediation; and

(7) providing information and recommendations on security and resilience measures to Federal and non-Federal entities, including information and recommendations to—

(A) facilitate information security; and

(B) strengthen information systems against cybersecurity risks and incidents.

**(d) Composition**

**(1) In general**

The Center shall be composed of—

(A) appropriate representatives of Federal entities, such as—

(i) sector-specific agencies;

(ii) civilian and law enforcement agencies; and

(iii) elements of the intelligence community, as that term is defined under section 3003(4) of title 50;

(B) appropriate representatives of non-Federal entities, such as—

(i) State and local governments;

(ii) information sharing and analysis organizations; and

(iii) owners and operators of critical information systems;

(C) components within the Center that carry out cybersecurity and communications activities;

(D) a designated Federal official for operational coordination with and across each sector; and

(E) other appropriate representatives or entities, as determined by the Secretary.

**(2) Incidents**

In the event of an incident, during exigent circumstances the Secretary may grant a Federal or non-Federal entity immediate temporary access to the Center.

**(e) Principles**

In carrying out the functions under subsection (c), the Center shall ensure—

(1) to the extent practicable, that—

(A) timely, actionable, and relevant information related to cybersecurity risks, incidents, and analysis is shared;

(B) when appropriate, information related to cybersecurity risks, incidents, and analysis is integrated with other relevant information and tailored to the specific characteristics of a sector;

(C) activities are prioritized and conducted based on the level of risk;

(D) industry sector-specific, academic, and national laboratory expertise is sought and receives appropriate consideration;

(E) continuous, collaborative, and inclusive coordination occurs—

(i) across sectors; and

(ii) with—

(I) sector coordinating councils;

(II) information sharing and analysis organizations; and

(III) other appropriate non-Federal partners;

(F) as appropriate, the Center works to develop and use mechanisms for sharing information related to cybersecurity risks and incidents that are technology-neutral, interoperable, real-time, cost-effective, and resilient; and

(G) the Center works with other agencies to reduce unnecessarily duplicative sharing of information related to cybersecurity risks and incidents;

(2) that information related to cybersecurity risks and incidents is appropriately safeguarded against unauthorized access; and

(3) that activities conducted by the Center comply with all policies, regulations, and laws that protect the privacy and civil liberties of United States persons.

**(f) No right or benefit**

**(1) In general**

The provision of assistance or information to, and inclusion in the Center of, governmental or private entities under this section shall be at the sole and unreviewable discretion of the Under Secretary appointed under section 113(a)(1)(H) of this title.

**(2) Certain assistance or information**

The provision of certain assistance or information to, or inclusion in the Center of, one governmental or private entity pursuant to this section shall not create a right or benefit, substantive or procedural, to similar assistance or information for any other governmental or private entity.

(Pub. L. 107–296, title II, § 226, as added Pub. L. 113–282, § 3(a), Dec. 18, 2014, 128 Stat. 3066.)

CODIFICATION

Another section 226 of Pub. L. 107–296 is classified to section 147 of this title.

RULES OF CONSTRUCTION

Pub. L. 113–282, § 8, Dec. 18, 2014, 128 Stat. 3072, provided that:

''(a) PROHIBITION ON NEW REGULATORY AUTHORITY.—Nothing in this Act [see section 1 of Pub. L. 113–282, set out as a Short Title of 2014 Amendment note under section 101 of this title] or the amendments made by this Act shall be construed to grant the Secretary [of Homeland Security] any authority to promulgate regulations or set standards relating to the cybersecurity of private sector critical infrastructure that was not in effect on the day before the date of enactment of this Act [Dec. 18, 2014].

''(b) PRIVATE ENTITIES.—Nothing in this Act or the amendments made by this Act shall be construed to require any private entity—

''(1) to request assistance from the Secretary; or

''(2) that requested such assistance from the Secretary to implement any measure or recommendation suggested by the Secretary.''

DEFINITIONS

Pub. L. 113–282, § 2, Dec. 18, 2014, 128 Stat. 3066, provided that: ''In this Act [see section 1 of Pub. L. 113–282, set out as a Short Title of 2014 Amendment note under section 101 of this title]—

''(1) the term 'Center' means the national cybersecurity and communications integration center under section 226 of the Homeland Security Act of 2002 [6 U.S.C. 148], as added by section 3;

''(2) the term 'critical infrastructure' has the meaning given that term in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101);

''(3) the term 'cybersecurity risk' has the meaning given that term in section 226 of the Homeland Security Act of 2002, as added by section 3;

''(4) the term 'information sharing and analysis organization' has the meaning given that term in section 212(5) of the Homeland Security Act of 2002 (6 U.S.C. 131(5));

''(5) the term 'information system' has the meaning given that term in section 3502(8) of title 44, United States Code; and

''(6) the term 'Secretary' means the Secretary of Homeland Security.''

## § 149. Cyber incident response plan

The Under Secretary appointed under section 113(a)(1)(H) of this title shall, in coordination with appropriate Federal departments and agencies, State and local governments, sector coordinating councils, information sharing and analysis organizations (as defined in section 131(5) of this title), owners and operators of critical infrastructure, and other appropriate entities and individuals, develop, regularly update, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks (as defined in section 148[1] of this title) to critical infrastructure.

(Pub. L. 107–296, title II, § 227, as added Pub. L. 113–282, § 7(a), Dec. 18, 2014, 128 Stat. 3070.)

REFERENCES IN TEXT

Section 148 of this title, referred to in text, was in the original ''section 226'' and was translated as meaning the section 226 of Pub. L. 107–296 as added by section 3(a) of Pub. L. 113–282, which is classified to section 148 of this title and defines ''cybersecurity risk''. Another section 226 of Pub. L. 107–296, as added by Pub. L. 113–277, is classified to section 147 of this title.

RULE OF CONSTRUCTION

Pub. L. 113–282, § 7(c), Dec. 18, 2014, 128 Stat. 3072, provided that: ''Nothing in the amendment made by subsection (a) [enacting this section and section 150 of this title] or in subsection (b)(1) [formerly classified as a note under section 3543 of Title 44, Public Printing and Documents, see now section 2(d)(1) of Pub. L. 113–283, set out as a note under section 3553 of Title 44] shall be construed to alter any authority of a Federal agency or department.''

## § 150. Clearances

The Secretary shall make available the process of application for security clearances under

[1] See References in Text note below.