

igned under section 132 of this title, to enter into a voluntary agreement to promote critical infrastructure security, including with any Information Sharing and Analysis Organization, or a plan of action as otherwise defined in section 4558 of title 50.

(Pub. L. 107–296, title II, §214, Nov. 25, 2002, 116 Stat. 2152; Pub. L. 108–271, §8(b), July 7, 2004, 118 Stat. 814; Pub. L. 112–199, title I, §111, Nov. 27, 2012, 126 Stat. 1472.)

REFERENCES IN TEXT

The Critical Infrastructure Information Act of 2002, referred to in subsec. (a)(2)(A), is subtitle B (§211 et seq.) of title II of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2150, which is classified generally to this part. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

The Federal Advisory Committee Act, referred to in subsec. (b), is Pub. L. 92–463, Oct. 6, 1972, 86 Stat. 770, as amended, which is set out in the Appendix to Title 5, Government Organization and Employees.

AMENDMENTS

2012—Subsec. (c). Pub. L. 112–199 inserted at end “For purposes of this section a permissible use of independently obtained information includes the disclosure of such information under section 2302(b)(8) of title 5.”

2004—Subsec. (a)(1)(D)(ii)(II). Pub. L. 108–271 substituted “Government Accountability Office” for “General Accounting Office”.

EFFECTIVE DATE OF 2012 AMENDMENT

Amendment by Pub. L. 112–199 effective 30 days after Nov. 27, 2012, see section 202 of Pub. L. 112–199, set out as a note under section 1204 of Title 5, Government Organization and Employees.

§ 134. No private right of action

Nothing in this part may be construed to create a private right of action for enforcement of any provision of this chapter.

(Pub. L. 107–296, title II, §215, Nov. 25, 2002, 116 Stat. 2155.)

REFERENCES IN TEXT

This chapter, referred to in text, was in the original “this Act”, meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

PART C—INFORMATION SECURITY

§ 141. Procedures for sharing information

The Secretary shall establish procedures on the use of information shared under this subchapter that—

- (1) limit the dissemination of such information to ensure that it is not used for an unauthorized purpose;
- (2) ensure the security and confidentiality of such information;
- (3) protect the constitutional and statutory rights of any individuals who are subjects of such information; and
- (4) provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.

(Pub. L. 107–296, title II, §221, Nov. 25, 2002, 116 Stat. 2155.)

REFERENCES IN TEXT

This subchapter, referred to in text, was in the original “this title”, meaning title II of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2145, which enacted this subchapter, amended sections 1030, 2511, 2512, 2520, 2701 to 2703, and 3125 of Title 18, Crimes and Criminal Procedure, sections 3712 and 3722 of Title 42, The Public Health and Welfare, and section 401a of Title 50, War and National Defense, and enacted provisions set out as a note under section 101 of this title and listed in a Provisions for Review, Promulgation, or Amendment of Federal Sentencing Guidelines Relating to Specific Offenses table set out under section 994 of Title 28, Judiciary and Judicial Procedure. For complete classification of title II to the Code, see Tables.

§ 142. Privacy officer

(a) Appointment and responsibilities

The Secretary shall appoint a senior official in the Department, who shall report directly to the Secretary, to assume primary responsibility for privacy policy, including—

(1) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;

(2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974 [5 U.S.C. 552a];

(3) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;

(4) conducting a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected;

(5) coordinating with the Officer for Civil Rights and Civil Liberties to ensure that—

(A) programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner; and

(B) Congress receives appropriate reports on such programs, policies, and procedures; and

(6) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974 [5 U.S.C. 552a], internal controls, and other matters.

(b) Authority to investigate

(1) In general

The senior official appointed under subsection (a) may—

(A) have access to all records, reports, audits, reviews, documents, papers, recommendations, and other materials available to the Department that relate to programs and operations with respect to the responsibilities of the senior official under this section;

(B) make such investigations and reports relating to the administration of the programs and operations of the Department as

are, in the senior official's judgment, necessary or desirable;

(C) subject to the approval of the Secretary, require by subpoena the production, by any person other than a Federal agency, of all information, documents, reports, answers, records, accounts, papers, and other data and documentary evidence necessary to performance of the responsibilities of the senior official under this section; and

(D) administer to or take from any person an oath, affirmation, or affidavit, whenever necessary to performance of the responsibilities of the senior official under this section.

(2) Enforcement of subpoenas

Any subpoena issued under paragraph (1)(C) shall, in the case of contumacy or refusal to obey, be enforceable by order of any appropriate United States district court.

(3) Effect of oaths

Any oath, affirmation, or affidavit administered or taken under paragraph (1)(D) by or before an employee of the Privacy Office designated for that purpose by the senior official appointed under subsection (a) shall have the same force and effect as if administered or taken by or before an officer having a seal of office.

(c) Supervision and coordination

(1) In general

The senior official appointed under subsection (a) shall—

(A) report to, and be under the general supervision of, the Secretary; and

(B) coordinate activities with the Inspector General of the Department in order to avoid duplication of effort.

(2) Coordination with the Inspector General

(A) In general

Except as provided in subparagraph (B), the senior official appointed under subsection (a) may investigate any matter relating to possible violations or abuse concerning the administration of any program or operation of the Department relevant to the purposes under this section.

(B) Coordination

(i) Referral

Before initiating any investigation described under subparagraph (A), the senior official shall refer the matter and all related complaints, allegations, and information to the Inspector General of the Department.

(ii) Determinations and notifications by the Inspector General

(I) In general

Not later than 30 days after the receipt of a matter referred under clause (i), the Inspector General shall—

(aa) make a determination regarding whether the Inspector General intends to initiate an audit or investigation of the matter referred under clause (i); and

(bb) notify the senior official of that determination.

(II) Investigation not initiated

If the Inspector General notifies the senior official under subclause (I)(bb) that the Inspector General intended to initiate an audit or investigation, but does not initiate that audit or investigation within 90 days after providing that notification, the Inspector General shall further notify the senior official that an audit or investigation was not initiated. The further notification under this subclause shall be made not later than 3 days after the end of that 90-day period.

(iii) Investigation by senior official

The senior official may investigate a matter referred under clause (i) if—

(I) the Inspector General notifies the senior official under clause (ii)(I)(bb) that the Inspector General does not intend to initiate an audit or investigation relating to that matter; or

(II) the Inspector General provides a further notification under clause (ii)(II) relating to that matter.

(iv) Privacy training

Any employee of the Office of Inspector General who audits or investigates any matter referred under clause (i) shall be required to receive adequate training on privacy laws, rules, and regulations, to be provided by an entity approved by the Inspector General in consultation with the senior official appointed under subsection (a).

(d) Notification to Congress on removal

If the Secretary removes the senior official appointed under subsection (a) or transfers that senior official to another position or location within the Department, the Secretary shall—

(1) promptly submit a written notification of the removal or transfer to Houses of Congress; and

(2) include in any such notification the reasons for the removal or transfer.

(e) Reports by senior official to Congress

The senior official appointed under subsection (a) shall—

(1) submit reports directly to the Congress regarding performance of the responsibilities of the senior official under this section, without any prior comment or amendment by the Secretary, Deputy Secretary, or any other officer or employee of the Department or the Office of Management and Budget; and

(2) inform the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives not later than—

(A) 30 days after the Secretary disapproves the senior official's request for a subpoena under subsection (b)(1)(C) or the Secretary substantively modifies the requested subpoena; or

(B) 45 days after the senior official's request for a subpoena under subsection (b)(1)(C), if that subpoena has not either been approved or disapproved by the Secretary.

(Pub. L. 107–296, title II, § 222, Nov. 25, 2002, 116 Stat. 2156; Pub. L. 108–458, title VIII, § 8305, Dec. 17, 2004, 118 Stat. 3868; Pub. L. 110–53, title VIII, § 802, Aug. 3, 2007, 121 Stat. 358.)

REFERENCES IN TEXT

The Privacy Act of 1974, referred to in subsec. (a)(2), (6), is Pub. L. 93–579, Dec. 31, 1974, 88 Stat. 1896, as amended, which enacted section 552a of Title 5, Government Organization and Employees, and provisions set out as notes under section 552a of Title 5. For complete classification of this Act to the Code, see Short Title of 1974 Amendment note set out under section 552a of Title 5 and Tables.

AMENDMENTS

2007—Pub. L. 110–53 designated existing provisions as subsec. (a), inserted heading, and added subsecs. (b) to (e).

2004—Pub. L. 108–458, § 8305(1), inserted “, who shall report directly to the Secretary,” after “in the Department” in introductory provisions.

Pars. (5), (6). Pub. L. 108–458, § 8305(2)–(4), added par. (5) and redesignated former par. (5) as (6).

§ 143. Enhancement of Federal and non-Federal cybersecurity

In carrying out the responsibilities under section 121 of this title, the Under Secretary appointed under section 113(a)(1)(H) of this title shall—

(1) as appropriate, provide to State and local government entities, and upon request to private entities that own or operate critical information systems—

(A) analysis and warnings related to threats to, and vulnerabilities of, critical information systems; and

(B) in coordination with the Under Secretary for Emergency Preparedness and Response, crisis management support in response to threats to, or attacks on, critical information systems; and

(2) as appropriate, provide technical assistance, upon request, to the private sector and other government entities, in coordination with the Under Secretary for Emergency Preparedness and Response, with respect to emergency recovery plans to respond to major failures of critical information systems; and

(3) fulfill the responsibilities of the Secretary to protect Federal information systems under subchapter II of chapter 35 of title 44.

(Pub. L. 107–296, title II, § 223, Nov. 25, 2002, 116 Stat. 2156; Pub. L. 110–53, title V, § 531(b)(1)(A), Aug. 3, 2007, 121 Stat. 334; Pub. L. 113–283, § 2(e)(3)(A), Dec. 18, 2014, 128 Stat. 3086.)

AMENDMENTS

2014—Pub. L. 113–283, § 2(e)(3)(A)(i), (ii), inserted “Federal and” before “non-Federal” in section catchline and substituted “the Under Secretary appointed under section 113(a)(1)(H) of this title” for “the Under Secretary for Intelligence and Analysis, in cooperation with the Assistant Secretary for Infrastructure Protection” in introductory provisions.

Par. (3). Pub. L. 113–283, § 2(e)(3)(A)(iii), (iv), added par. (3).

2007—Pub. L. 110–53 substituted “Under Secretary for Intelligence and Analysis, in cooperation with the Assistant Secretary for Infrastructure Protection” for “Under Secretary for Information Analysis and Infrastructure Protection” in introductory provisions.

§ 144. NET Guard

The Assistant Secretary for Infrastructure Protection may establish a national technology guard, to be known as “NET Guard”, comprised of local teams of volunteers with expertise in relevant areas of science and technology, to assist local communities to respond and recover from attacks on information systems and communications networks.

(Pub. L. 107–296, title II, § 224, Nov. 25, 2002, 116 Stat. 2156; Pub. L. 110–53, title V, § 531(b)(1)(B), Aug. 3, 2007, 121 Stat. 334.)

AMENDMENTS

2007—Pub. L. 110–53 substituted “Assistant Secretary for Infrastructure Protection” for “Under Secretary for Information Analysis and Infrastructure Protection”.

§ 145. Cyber Security Enhancement Act of 2002

(a) Short title

This section may be cited as the “Cyber Security Enhancement Act of 2002”.

(b) Amendment of sentencing guidelines relating to certain computer crimes

(1) Directive to the United States Sentencing Commission

Pursuant to its authority under section 994(p) of title 28 and in accordance with this subsection, the United States Sentencing Commission shall review and, if appropriate, amend its guidelines and its policy statements applicable to persons convicted of an offense under section 1030 of title 18.

(2) Requirements

In carrying out this subsection, the Sentencing Commission shall—

(A) ensure that the sentencing guidelines and policy statements reflect the serious nature of the offenses described in paragraph (1), the growing incidence of such offenses, and the need for an effective deterrent and appropriate punishment to prevent such offenses;

(B) consider the following factors and the extent to which the guidelines may or may not account for them—

(i) the potential and actual loss resulting from the offense;

(ii) the level of sophistication and planning involved in the offense;

(iii) whether the offense was committed for purposes of commercial advantage or private financial benefit;

(iv) whether the defendant acted with malicious intent to cause harm in committing the offense;

(v) the extent to which the offense violated the privacy rights of individuals harmed;

(vi) whether the offense involved a computer used by the government in furtherance of national defense, national security, or the administration of justice;

(vii) whether the violation was intended to or had the effect of significantly interfering with or disrupting a critical infrastructure; and

(viii) whether the violation was intended to or had the effect of creating a threat to

public health or safety, or injury to any person;

(C) assure reasonable consistency with other relevant directives and with other sentencing guidelines;

(D) account for any additional aggravating or mitigating circumstances that might justify exceptions to the generally applicable sentencing ranges;

(E) make any necessary conforming changes to the sentencing guidelines; and

(F) assure that the guidelines adequately meet the purposes of sentencing as set forth in section 3553(a)(2) of title 18.

(c) Study and report on computer crimes

Not later than May 1, 2003, the United States Sentencing Commission shall submit a brief report to Congress that explains any actions taken by the Sentencing Commission in response to this section and includes any recommendations the Commission may have regarding statutory penalties for offenses under section 1030 of title 18.

(d) Emergency disclosure exception

(1) Omitted

(2) Reporting of disclosures

A government entity that receives a disclosure under section 2702(b) of title 18 shall file, not later than 90 days after such disclosure, a report to the Attorney General stating the paragraph of that section under which the disclosure was made, the date of the disclosure, the entity to which the disclosure was made, the number of customers or subscribers to whom the information disclosed pertained, and the number of communications, if any, that were disclosed. The Attorney General shall publish all such reports into a single report to be submitted to Congress 1 year after November 25, 2002.

(Pub. L. 107–296, title II, § 225, Nov. 25, 2002, 116 Stat. 2156.)

CODIFICATION

Section is comprised of section 225 of Pub. L. 107–296. Subsecs. (d)(1) and (e) to (j) of section 225 of Pub. L. 107–296 amended sections 1030, 2511, 2512, 2520, 2701 to 2703, and 3125 of Title 18, Crimes and Criminal Procedure.

§ 146. Cybersecurity workforce assessment and strategy

(a) Workforce assessment

(1) In general

Not later than 180 days after December 18, 2014, and annually thereafter for 3 years, the Secretary shall assess the cybersecurity workforce of the Department.

(2) Contents

The assessment required under paragraph (1) shall include, at a minimum—

(A) an assessment of the readiness and capacity of the workforce of the Department to meet its cybersecurity mission;

(B) information on where cybersecurity workforce positions are located within the Department;

(C) information on which cybersecurity workforce positions are—

(i) performed by—

(I) permanent full-time equivalent employees of the Department, including, to the greatest extent practicable, demographic information about such employees;

(II) independent contractors; and

(III) individuals employed by other Federal agencies, including the National Security Agency; or

(ii) vacant; and

(D) information on—

(i) the percentage of individuals within each Cybersecurity Category and Specialty Area who received essential training to perform their jobs; and

(ii) in cases in which such essential training was not received, what challenges, if any, were encountered with respect to the provision of such essential training.

(b) Workforce strategy

(1) In general

The Secretary shall—

(A) not later than 1 year after December 18, 2014, develop a comprehensive workforce strategy to enhance the readiness, capacity, training, recruitment, and retention of the cybersecurity workforce of the Department; and

(B) maintain and, as necessary, update the comprehensive workforce strategy developed under subparagraph (A).

(2) Contents

The comprehensive workforce strategy developed under paragraph (1) shall include a description of—

(A) a multi-phased recruitment plan, including with respect to experienced professionals, members of disadvantaged or underserved communities, the unemployed, and veterans;

(B) a 5-year implementation plan;

(C) a 10-year projection of the cybersecurity workforce needs of the Department;

(D) any obstacle impeding the hiring and development of a cybersecurity workforce in the Department; and

(E) any gap in the existing cybersecurity workforce of the Department and a plan to fill any such gap.

(c) Updates

The Secretary submit¹ to the appropriate congressional committees annual updates on—

(1) the cybersecurity workforce assessment required under subsection (a); and

(2) the progress of the Secretary in carrying out the comprehensive workforce strategy required to be developed under subsection (b).

(Pub. L. 113–246, § 3, Dec. 18, 2014, 128 Stat. 2880.)

CODIFICATION

Section was enacted as part of the Cybersecurity Workforce Assessment Act, and not as part of the

¹ So in original.

Homeland Security Act of 2002 which comprises this chapter.

HOMELAND SECURITY CYBERSECURITY WORKFORCE
ASSESSMENT

Pub. L. 113-277, § 4, Dec. 18, 2014, 128 Stat. 3008, provided that:

“(a) **SHORT TITLE.**—This section may be cited as the ‘Homeland Security Cybersecurity Workforce Assessment Act’.

“(b) **DEFINITIONS.**—In this section:

“(1) **APPROPRIATE CONGRESSIONAL COMMITTEES.**—The term ‘appropriate congressional committees’ means—

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

“(B) the Committee on Homeland Security of the House of Representatives; and

“(C) the Committee on House Administration of the House of Representatives.

“(2) **CYBERSECURITY WORK CATEGORY; DATA ELEMENT CODE; SPECIALTY AREA.**—The terms ‘Cybersecurity Work Category’, ‘Data Element Code’, and ‘Specialty Area’ have the meanings given such terms in the Office of Personnel Management’s Guide to Data Standards.

“(3) **DEPARTMENT.**—The term ‘Department’ means the Department of Homeland Security.

“(4) **DIRECTOR.**—The term ‘Director’ means the Director of the Office of Personnel Management.

“(5) **SECRETARY.**—The term ‘Secretary’ means the Secretary of Homeland Security.

“(c) **NATIONAL CYBERSECURITY WORKFORCE MEASUREMENT INITIATIVE.**—

“(1) **IN GENERAL.**—The Secretary shall—

“(A) identify all cybersecurity workforce positions within the Department;

“(B) determine the primary Cybersecurity Work Category and Specialty Area of such positions; and

“(C) assign the corresponding Data Element Code, as set forth in the Office of Personnel Management’s Guide to Data Standards which is aligned with the National Initiative for Cybersecurity Education’s National Cybersecurity Workforce Framework report, in accordance with paragraph (2).

“(2) **EMPLOYMENT CODES.**—

“(A) **PROCEDURES.**—Not later than 90 days after the date of the enactment of this Act [Dec. 18, 2014], the Secretary shall establish procedures—

“(i) to identify open positions that include cybersecurity functions (as defined in the OPM Guide to Data Standards); and

“(ii) to assign the appropriate employment code to each such position, using agreed standards and definitions.

“(B) **CODE ASSIGNMENTS.**—Not later than 9 months after the date of the enactment of this Act, the Secretary shall assign the appropriate employment code to—

“(i) each employee within the Department who carries out cybersecurity functions; and

“(ii) each open position within the Department that have been identified as having cybersecurity functions.

“(3) **PROGRESS REPORT.**—Not later than 1 year after the date of the enactment of this Act, the Director shall submit a progress report on the implementation of this subsection to the appropriate congressional committees.

“(d) **IDENTIFICATION OF CYBERSECURITY SPECIALTY AREAS OF CRITICAL NEED.**—

“(1) **IN GENERAL.**—Beginning not later than 1 year after the date on which the employment codes are assigned to employees pursuant to subsection (c)(2)(B), and annually through 2021, the Secretary, in consultation with the Director, shall—

“(A) identify Cybersecurity Work Categories and Specialty Areas of critical need in the Department’s cybersecurity workforce; and

“(B) submit a report to the Director that—

“(i) describes the Cybersecurity Work Categories and Specialty Areas identified under subparagraph (A); and

“(ii) substantiates the critical need designations.

“(2) **GUIDANCE.**—The Director shall provide the Secretary with timely guidance for identifying Cybersecurity Work Categories and Specialty Areas of critical need, including—

“(A) current Cybersecurity Work Categories and Specialty Areas with acute skill shortages; and

“(B) Cybersecurity Work Categories and Specialty Areas with emerging skill shortages.

“(3) **CYBERSECURITY CRITICAL NEEDS REPORT.**—Not later than 18 months after the date of the enactment of this Act, the Secretary, in consultation with the Director, shall—

“(A) identify Specialty Areas of critical need for cybersecurity workforce across the Department; and

“(B) submit a progress report on the implementation of this subsection to the appropriate congressional committees.

“(e) **GOVERNMENT ACCOUNTABILITY OFFICE STATUS REPORTS.**—The Comptroller General of the United States shall—

“(1) analyze and monitor the implementation of subsections (c) and (d); and

“(2) not later than 3 years after the date of the enactment of this Act, submit a report to the appropriate congressional committees that describes the status of such implementation.”

DEFINITIONS

Pub. L. 113-246, § 2, Dec. 18, 2014, 128 Stat. 2880, provided that: “In this Act [enacting this section and provisions set out as a note under section 101 of this title]—

“(1) the term ‘Cybersecurity Category’ means a position’s or incumbent’s primary work function involving cybersecurity, which is further defined by Specialty Area;

“(2) the term ‘Department’ means the Department of Homeland Security;

“(3) the term ‘Secretary’ means the Secretary of Homeland Security; and

“(4) the term ‘Specialty Area’ means any of the common types of cybersecurity work as recognized by the National Initiative for Cybersecurity Education’s National Cybersecurity Workforce Framework report.”

§ 147. Cybersecurity recruitment and retention

(a) **Definitions**

In this section:

(1) **Appropriate committees of Congress**

The term “appropriate committees of Congress” means the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives.

(2) **Collective bargaining agreement**

The term “collective bargaining agreement” has the meaning given that term in section 7103(a)(8) of title 5.

(3) **Excepted service**

The term “excepted service” has the meaning given that term in section 2103 of title 5.

(4) **Preference eligible**

The term “preference eligible” has the meaning given that term in section 2108 of title 5.

(5) **Qualified position**

The term “qualified position” means a position, designated by the Secretary for the pur-

pose of this section, in which the incumbent performs, manages, or supervises functions that execute the responsibilities of the Department relating to cybersecurity.

(6) Senior Executive Service

The term “Senior Executive Service” has the meaning given that term in section 2101a of title 5.

(b) General authority

(1) Establish positions, appoint personnel, and fix rates of pay

(A) General authority

The Secretary may—

(i) establish, as positions in the excepted service, such qualified positions in the Department as the Secretary determines necessary to carry out the responsibilities of the Department relating to cybersecurity, including positions formerly identified as—

(I) senior level positions designated under section 5376 of title 5; and

(II) positions in the Senior Executive Service;

(ii) appoint an individual to a qualified position (after taking into consideration the availability of preference eligibles for appointment to the position); and

(iii) subject to the requirements of paragraphs (2) and (3), fix the compensation of an individual for service in a qualified position.

(B) Construction with other laws

The authority of the Secretary under this subsection applies without regard to the provisions of any other law relating to the appointment, number, classification, or compensation of employees.

(2) Basic pay

(A) Authority to fix rates of basic pay

In accordance with this section, the Secretary shall fix the rates of basic pay for any qualified position established under paragraph (1) in relation to the rates of pay provided for employees in comparable positions in the Department of Defense and subject to the same limitations on maximum rates of pay established for such employees by law or regulation.

(B) Prevailing rate systems

The Secretary may, consistent with section 5341 of title 5, adopt such provisions of that title as provide for prevailing rate systems of basic pay and may apply those provisions to qualified positions for employees in or under which the Department may employ individuals described by section 5342(a)(2)(A) of that title.

(3) Additional compensation, incentives, and allowances

(A) Additional compensation based on title 5 authorities

The Secretary may provide employees in qualified positions compensation (in addition to basic pay), including benefits, incen-

tives, and allowances, consistent with, and not in excess of the level authorized for, comparable positions authorized by title 5.

(B) Allowances in nonforeign areas

An employee in a qualified position whose rate of basic pay is fixed under paragraph (2)(A) shall be eligible for an allowance under section 5941 of title 5, on the same basis and to the same extent as if the employee was an employee covered by such section 5941, including eligibility conditions, allowance rates, and all other terms and conditions in law or regulation.

(4) Plan for execution of authorities

Not later than 120 days after December 18, 2014, the Secretary shall submit a report to the appropriate committees of Congress with a plan for the use of the authorities provided under this subsection.

(5) Collective bargaining agreements

Nothing in paragraph (1) may be construed to impair the continued effectiveness of a collective bargaining agreement with respect to an office, component, subcomponent, or equivalent of the Department that is a successor to an office, component, subcomponent, or equivalent of the Department covered by the agreement before the succession.

(6) Required regulations

The Secretary, in coordination with the Director of the Office of Personnel Management, shall prescribe regulations for the administration of this section.

(c) Annual report

Not later than 1 year after December 18, 2014, and every year thereafter for 4 years, the Secretary shall submit to the appropriate committees of Congress a detailed report that—

(1) discusses the process used by the Secretary in accepting applications, assessing candidates, ensuring adherence to veterans’ preference, and selecting applicants for vacancies to be filled by an individual for a qualified position;

(2) describes—

(A) how the Secretary plans to fulfill the critical need of the Department to recruit and retain employees in qualified positions;

(B) the measures that will be used to measure progress; and

(C) any actions taken during the reporting period to fulfill such critical need;

(3) discusses how the planning and actions taken under paragraph (2) are integrated into the strategic workforce planning of the Department;

(4) provides metrics on actions occurring during the reporting period, including—

(A) the number of employees in qualified positions hired by occupation and grade and level or pay band;

(B) the placement of employees in qualified positions by directorate and office within the Department;

(C) the total number of veterans hired;

(D) the number of separations of employees in qualified positions by occupation and grade and level or pay band;

(E) the number of retirements of employees in qualified positions by occupation and grade and level or pay band; and

(F) the number and amounts of recruitment, relocation, and retention incentives paid to employees in qualified positions by occupation and grade and level or pay band; and

(5) describes the training provided to supervisors of employees in qualified positions at the Department on the use of the new authorities.

(d) Three-year probationary period

The probationary period for all employees hired under the authority established in this section shall be 3 years.

(e) Incumbents of existing competitive service positions

(1) In general

An individual serving in a position on December 18, 2014, that is selected to be converted to a position in the excepted service under this section shall have the right to refuse such conversion.

(2) Subsequent conversion

After the date on which an individual who refuses a conversion under paragraph (1) stops serving in the position selected to be converted, the position may be converted to a position in the excepted service.

(f) Study and report

Not later than 120 days after December 18, 2014, the National Protection and Programs Directorate 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.)

§ 148. National cybersecurity and communications integration center

(a) Definitions

In this section—

(1) the term “cybersecurity risk”—

(A) 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 such information or information systems, including such related consequences caused by an act of terrorism; and

(B) does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement;

(2) the terms “cyber threat indicator” and “defensive measure” have the meanings given those terms in section 102 of the Cybersecurity Act of 2015 [6 U.S.C. 1501];

(3) the term “incident” means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system;

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

(5) the term “information system” has the meaning given that term in section 3502(8) of title 44; and

(6) the term “sharing” (including all conjugations thereof) means providing, receiving, and disseminating (including all conjugations of each of such terms).

(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 cyber threat indicators, defensive measures, cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities, including the implementation of title I of the Cybersecurity Act of 2015 [6 U.S.C. 1501 et seq.];

(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 cyber threat indicators, defensive measures, 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 cyber threat indicators, defensive measures, 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 cyber threat indicators, defensive measures, cybersecurity risks, and incidents, which may include attribution, mitigation, and remediation;

(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;
 - (B) strengthen information systems against cybersecurity risks and incidents; and
 - (C) sharing¹ cyber threat indicators and defensive measures;
- (8) engaging with international partners, in consultation with other appropriate agencies, to—
- (A) collaborate on cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents; and
 - (B) enhance the security and resilience of global cybersecurity;
- (9) sharing cyber threat indicators, defensive measures, and other information related to cybersecurity risks and incidents with Federal and non-Federal entities, including across sectors of critical infrastructure and with State and major urban area fusion centers, as appropriate;
- (10) participating, as appropriate, in national exercises run by the Department; and
- (11) in coordination with the Office of Emergency Communications of the Department, assessing and evaluating consequence, vulnerability, and threat information regarding cyber incidents to public safety communications to help facilitate continuous improvements to the security and resiliency of such communications.

(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, local, and tribal governments;
 - (ii) information sharing and analysis organizations, including information sharing and analysis centers;
 - (iii) owners and operators of critical information systems; and
 - (iv) private entities;
- (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;
- (E) an entity that collaborates with State and local governments on cybersecurity risks and incidents, and has entered into a voluntary information sharing relationship with the Center; and
- (F) other appropriate representatives or entities, as determined by the Secretary.

¹ So in original. Probably should be “share”.

(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 cyber threat indicators, defensive measures, and information related to cybersecurity risks, incidents, and analysis is shared;
 - (B) when appropriate, cyber threat indicators, defensive measures, and 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 cyber threat indicators, defensive measures, cybersecurity risks, and incidents that are technology-neutral, interoperable, real-time, cost-effective, and resilient;

(G) the Center works with other agencies to reduce unnecessarily duplicative sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents; and²

(H) the Center designates an agency contact for non-Federal entities;

(2) that information related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents is appropriately safeguarded against unauthorized access or disclosure; 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, including by working with the Privacy Officer appointed under section 142 of this title to ensure that the Center follows the policies and procedures specified in subsections (b) and (d)(5)(C) of section 105 of the Cybersecurity Act of 2015 [6 U.S.C. 1504].

(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

² So in original. The semicolon probably should not appear.

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.

(g) Automated information sharing

(1) In general

The Under Secretary appointed under section 113(a)(1)(H) of this title, in coordination with industry and other stakeholders, shall develop capabilities making use of existing information technology industry standards and best practices, as appropriate, that support and rapidly advance the development, adoption, and implementation of automated mechanisms for the sharing of cyber threat indicators and defensive measures in accordance with title I of the Cybersecurity Act of 2015 [6 U.S.C. 1501 et seq.].

(2) Annual report

The Under Secretary appointed under section 113(a)(1)(H) of this title shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives an annual report on the status and progress of the development of the capabilities described in paragraph (1). Such reports shall be required until such capabilities are fully implemented.

(h) Voluntary information sharing procedures

(1) Procedures

(A) In general

The Center may enter into a voluntary information sharing relationship with any consenting non-Federal entity for the sharing of cyber threat indicators and defensive measures for cybersecurity purposes in accordance with this section. Nothing in this subsection may be construed to require any non-Federal entity to enter into any such information sharing relationship with the Center or any other entity. The Center may terminate a voluntary information sharing relationship under this subsection, at the sole and unreviewable discretion of the Secretary, acting through the Under Secretary appointed under section 113(a)(1)(H) of this title, for any reason, including if the Center determines that the non-Federal entity with which the Center has entered into such a relationship has violated the terms of this subsection.

(B) National security

The Secretary may decline to enter into a voluntary information sharing relationship under this subsection, at the sole and unreviewable discretion of the Secretary, acting through the Under Secretary appointed under section 113(a)(1)(H) of this title, for any reason, including if the Secretary deter-

mines that such is appropriate for national security.

(2) Voluntary information sharing relationships

A voluntary information sharing relationship under this subsection may be characterized as an agreement described in this paragraph.

(A) Standard agreement

For the use of a non-Federal entity, the Center shall make available a standard agreement, consistent with this section, on the Department's website.

(B) Negotiated agreement

At the request of a non-Federal entity, and if determined appropriate by the Center, at the sole and unreviewable discretion of the Secretary, acting through the Under Secretary appointed under section 113(a)(1)(H) of this title, the Department shall negotiate a non-standard agreement, consistent with this section.

(C) Existing agreements

An agreement between the Center and a non-Federal entity that is entered into before December 18, 2015, or such an agreement that is in effect before such date, shall be deemed in compliance with the requirements of this subsection, notwithstanding any other provision or requirement of this subsection. An agreement under this subsection shall include the relevant privacy protections as in effect under the Cooperative Research and Development Agreement for Cybersecurity Information Sharing and Collaboration, as of December 31, 2014. Nothing in this subsection may be construed to require a non-Federal entity to enter into either a standard or negotiated agreement to be in compliance with this subsection.

(i) Direct reporting

The Secretary shall develop policies and procedures for direct reporting to the Secretary by the Director of the Center regarding significant cybersecurity risks and incidents.

(j) Reports on international cooperation

Not later than 180 days after December 18, 2015, and periodically thereafter, the Secretary of Homeland Security shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the range of efforts underway to bolster cybersecurity collaboration with relevant international partners in accordance with subsection (c)(8).

(k) Outreach

Not later than 60 days after December 18, 2015, the Secretary, acting through the Under Secretary appointed under section 113(a)(1)(H) of this title, shall—

(1) disseminate to the public information about how to voluntarily share cyber threat indicators and defensive measures with the Center; and

(2) enhance outreach to critical infrastructure owners and operators for purposes of such sharing.

(I) Coordinated vulnerability disclosure

The Secretary, in coordination with industry and other stakeholders, may develop and adhere to Department policies and procedures for coordinating vulnerability disclosures.

(Pub. L. 107–296, title II, § 227, formerly § 226, as added Pub. L. 113–282, § 3(a), Dec. 18, 2014, 128 Stat. 3066; renumbered § 227 and amended Pub. L. 114–113, div. N, title II, §§ 203, 223(a)(3), Dec. 18, 2015, 129 Stat. 2957, 2963.)

REFERENCES IN TEXT

Title I of the Cybersecurity Act of 2015, referred to in subsecs. (c)(1) and (g)(1), is title I of Pub. L. 114–113, div. N, Dec. 18, 2015, 129 Stat. 2936, also known as the Cybersecurity Information Sharing Act of 2015, which is classified generally to subchapter I of chapter 6 of this title. For complete classification of title I to the Code, see Short Title note set out under section 1501 of this title and Tables.

PRIOR PROVISIONS

A prior section 227 of Pub. L. 107–296, as added by Pub. L. 113–282, § 7(a), Dec. 18, 2014, 128 Stat. 3070, was classified to section 149 of this title prior to redesignation by Pub. L. 114–113 as section 228(c) of Pub. L. 107–296, which is now classified to section 149(c) of this title.

AMENDMENTS

2015—Subsec. (a)(1) to (5). Pub. L. 114–113, § 203(1)(A), (B), added pars. (1) to (3), redesignated former pars. (3) and (4) as (4) and (5), respectively, and struck out former pars. (1) and (2), which defined “cybersecurity risk” and “incident”, respectively.

Subsec. (a)(6). Pub. L. 114–113, § 203(1)(C)–(E), added par. (6).

Subsec. (c)(1). Pub. L. 114–113, § 203(2)(A), inserted “cyber threat indicators, defensive measures,” before “cybersecurity risks” and “, including the implementation of title I of the Cybersecurity Act of 2015” before semicolon at end.

Subsec. (c)(3). Pub. L. 114–113, § 203(2)(B), substituted “cyber threat indicators, defensive measures, cybersecurity risks,” for “cybersecurity risks”.

Subsec. (c)(5)(A). Pub. L. 114–113, § 203(2)(C), substituted “cyber threat indicators, defensive measures, cybersecurity risks,” for “cybersecurity risks”.

Subsec. (c)(6). Pub. L. 114–113, § 203(2)(D), substituted “cyber threat indicators, defensive measures, cybersecurity risks,” for “cybersecurity risks” and struck out “and” at end.

Subsec. (c)(7)(C). Pub. L. 114–113, § 203(2)(E), added subpar. (C).

Subsec. (c)(8) to (11). Pub. L. 114–113, § 203(2)(F), added pars. (8) to (11).

Subsec. (d)(1)(B)(i). Pub. L. 114–113, § 203(3)(A)(i), substituted “, local, and tribal” for “and local”.

Subsec. (d)(1)(B)(ii). Pub. L. 114–113, § 203(3)(A)(ii), substituted “, including information sharing and analysis centers;” for “; and”.

Subsec. (d)(1)(B)(iv). Pub. L. 114–113, § 203(3)(A)(iii), (iv), added cl. (iv).

Subsec. (d)(1)(E), (F). Pub. L. 114–113, § 203(3)(B)–(D), added subpar. (E) and redesignated former subpar. (E) as (F).

Subsec. (e)(1)(A). Pub. L. 114–113, § 203(4)(A)(i), inserted “cyber threat indicators, defensive measures, and” before “information”.

Subsec. (e)(1)(B). Pub. L. 114–113, § 203(4)(A)(ii), inserted “cyber threat indicators, defensive measures, and” before “information related”.

Subsec. (e)(1)(F). Pub. L. 114–113, § 203(4)(A)(iii), substituted “cyber threat indicators, defensive measures, cybersecurity risks,” for “cybersecurity risks” and struck out “and” at end.

Subsec. (e)(1)(G). Pub. L. 114–113, § 203(4)(A)(iv), substituted “cyber threat indicators, defensive measures,

cybersecurity risks, and incidents; and” for “cybersecurity risks and incidents”.

Subsec. (e)(1)(H). Pub. L. 114–113, § 203(4)(A)(v), added subpar. (H).

Subsec. (e)(2). Pub. L. 114–113, § 203(4)(B), substituted “cyber threat indicators, defensive measures, cybersecurity risks,” for “cybersecurity risks” and inserted “or disclosure” after “access”.

Subsec. (e)(3). Pub. L. 114–113, § 203(4)(C), inserted “, including by working with the Privacy Officer appointed under section 142 of this title to ensure that the Center follows the policies and procedures specified in subsections (b) and (d)(5)(C) of section 105 of the Cybersecurity Act of 2015” before period at end.

Subsecs. (g) to (I). Pub. L. 114–113, § 203(5), added subsecs. (g) to (I).

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 [renumbered 227 by section 223(a)(3) of Pub. L. 114–113] 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. Cybersecurity plans**(a) Definitions**

In this section—

(1) the term “agency information system” means an information system used or operated by an agency or by another entity on behalf of an agency;

(2) the terms “cybersecurity risk” and “information system” have the meanings given those terms in section 148 of this title;

(3) the term “intelligence community” has the meaning given the term in section 3003(4) of title 50; and

(4) the term “national security system” has the meaning given the term in section 11103 of title 40.

(b) Intrusion assessment plan

(1) Requirement

The Secretary, in coordination with the Director of the Office of Management and Budget, shall—

(A) develop and implement an intrusion assessment plan to proactively detect, identify, and remove intruders in agency information systems on a routine basis; and

(B) update such plan as necessary.

(2) Exception

The intrusion assessment plan required under paragraph (1) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

(c) 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 of this title) to critical infrastructure.

(d) National Response Framework

The Secretary, in coordination with the heads of other appropriate Federal departments and agencies, and in accordance with the National Cybersecurity Incident Response Plan required under subsection (c), shall regularly update, maintain, and exercise the Cyber Incident Annex to the National Response Framework of the Department.

(Pub. L. 107–296, title II, § 228, as added and amended Pub. L. 114–113, div. N, title II, §§ 205, 223(a)(2), (4), (5), Dec. 18, 2015, 129 Stat. 2961, 2963, 2964.)

CODIFICATION

Former section 149 of this title, which was transferred and redesignated as subsec. (c) of this section by Pub. L. 114–113, div. N, title II, § 223(a)(2), Dec. 18, 2015, 129 Stat. 2963, was based on Pub. L. 107–296, title II, § 227, as added by Pub. L. 113–282, § 7(a), Dec. 18, 2014, 128 Stat. 3070.

PRIOR PROVISIONS

A prior section 228 of Pub. L. 107–296 was renumbered section 229 and is classified to section 150 of this title.

AMENDMENTS

2015—Subsec. (c). Pub. L. 114–113, § 223(a)(5), made technical amendment to reference in original act which appears in text as reference to section 148 of this title.

Pub. L. 114–113, § 223(a)(2), transferred former section 149 of this title to subsec. (c) of this section. See Codification note above.

Subsec. (d). Pub. L. 114–113, § 205, added subsec. (d).

RULE OF CONSTRUCTION

Pub. L. 113–282, § 7(c), Dec. 18, 2014, 128 Stat. 3072, provided that: “Nothing in the amendment made by sub-

section (a) [enacting subsec. (c) of 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 Executive Order 13549 (75 Fed. Reg. 162;¹ relating to a classified national security information program) or any successor Executive Order to appropriate representatives of sector coordinating councils, sector information sharing and analysis organizations (as defined in section 131(5) of this title), owners and operators of critical infrastructure, and any other person that the Secretary determines appropriate.

(Pub. L. 107–296, title II, § 229, formerly § 228, as added Pub. L. 113–282, § 7(a), Dec. 18, 2014, 128 Stat. 3070; renumbered § 229, Pub. L. 114–113, div. N, title II, § 223(a)(1), Dec. 18, 2015, 129 Stat. 2963.)

REFERENCES IN TEXT

Executive Order 13549, referred to in text, is set out as a note under section 3161 of Title 50, War and National Defense.

§ 151. Federal intrusion detection and prevention system

(a) Definitions

In this section—

(1) the term “agency” has the meaning given the term in section 3502 of title 44;

(2) the term “agency information” means information collected or maintained by or on behalf of an agency;

(3) the term “agency information system” has the meaning given the term in section 149 of this title; and

(4) the terms “cybersecurity risk” and “information system” have the meanings given those terms in section 148 of this title.

(b) Requirement

(1) In general

Not later than 1 year after December 18, 2015, the Secretary shall deploy, operate, and maintain, to make available for use by any agency, with or without reimbursement—

(A) a capability to detect cybersecurity risks in network traffic transiting or traveling to or from an agency information system; and

(B) a capability to prevent network traffic associated with such cybersecurity risks from transiting or traveling to or from an agency information system or modify such network traffic to remove the cybersecurity risk.

(2) Regular improvement

The Secretary shall regularly deploy new technologies and modify existing technologies to the intrusion detection and prevention capabilities described in paragraph (1) as appropriate to improve the intrusion detection and prevention capabilities.

¹ So in original. Probably should be “51609”.

(c) Activities

In carrying out subsection (b), the Secretary—

(1) may access, and the head of an agency may disclose to the Secretary or a private entity providing assistance to the Secretary under paragraph (2), information transiting or traveling to or from an agency information system, regardless of the location from which the Secretary or a private entity providing assistance to the Secretary under paragraph (2) accesses such information, notwithstanding any other provision of law that would otherwise restrict or prevent the head of an agency from disclosing such information to the Secretary or a private entity providing assistance to the Secretary under paragraph (2);

(2) may enter into contracts or other agreements with, or otherwise request and obtain the assistance of, private entities to deploy, operate, and maintain technologies in accordance with subsection (b);

(3) may retain, use, and disclose information obtained through the conduct of activities authorized under this section only to protect information and information systems from cybersecurity risks;

(4) shall regularly assess through operational test and evaluation in real world or simulated environments available advanced protective technologies to improve detection and prevention capabilities, including commercial and noncommercial technologies and detection technologies beyond signature-based detection, and acquire, test, and deploy such technologies when appropriate;

(5) shall establish a pilot through which the Secretary may acquire, test, and deploy, as rapidly as possible, technologies described in paragraph (4); and

(6) shall periodically update the privacy impact assessment required under section 208(b) of the E-Government Act of 2002 (44 U.S.C. 3501 note).

(d) Principles

In carrying out subsection (b), the Secretary shall ensure that—

(1) activities carried out under this section are reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

(2) information accessed by the Secretary will be retained no longer than reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

(3) notice has been provided to users of an agency information system concerning access to communications of users of the agency information system for the purpose of protecting agency information and the agency information system; and

(4) the activities are implemented pursuant to policies and procedures governing the operation of the intrusion detection and prevention capabilities.

(e) Private entities**(1) Conditions**

A private entity described in subsection (c)(2) may not—

(A) disclose any network traffic transiting or traveling to or from an agency information system to any entity other than the Department or the agency that disclosed the information under subsection (c)(1), including personal information of a specific individual or information that identifies a specific individual not directly related to a cybersecurity risk; or

(B) use any network traffic transiting or traveling to or from an agency information system to which the private entity gains access in accordance with this section for any purpose other than to protect agency information and agency information systems against cybersecurity risks or to administer a contract or other agreement entered into pursuant to subsection (c)(2) or as part of another contract with the Secretary.

(2) Limitation on liability

No cause of action shall lie in any court against a private entity for assistance provided to the Secretary in accordance with this section and any contract or agreement entered into pursuant to subsection (c)(2).

(3) Rule of construction

Nothing in paragraph (2) shall be construed to authorize an Internet service provider to break a user agreement with a customer without the consent of the customer.

(f) Privacy Officer review

Not later than 1 year after December 18, 2015, the Privacy Officer appointed under section 142 of this title, in consultation with the Attorney General, shall review the policies and guidelines for the program carried out under this section to ensure that the policies and guidelines are consistent with applicable privacy laws, including those governing the acquisition, interception, retention, use, and disclosure of communications.

(Pub. L. 107–296, title II, § 230, as added Pub. L. 114–113, div. N, title II, § 223(a)(6), Dec. 18, 2015, 129 Stat. 2964.)

REFERENCES IN TEXT

Section 208(b) of the E-Government Act of 2002, referred to in subsec. (c)(6), is section 208(b) of title II of Pub. L. 107–347, which is set out in a note under section 3501 of Title 44, Public Printing and Documents.

AGENCY RESPONSIBILITIES

Pub. L. 114–113, div. N, title II, § 223(b), Dec. 18, 2015, 129 Stat. 2966, provided that:

“(1) IN GENERAL.—Except as provided in paragraph (2)—

“(A) not later than 1 year after the date of enactment of this Act [Dec. 18, 2015] or 2 months after the date on which the Secretary makes available the intrusion detection and prevention capabilities under section 230(b)(1) of the Homeland Security Act of 2002 [6 U.S.C. 151(b)(1)], as added by subsection (a), whichever is later, the head of each agency shall apply and continue to utilize the capabilities to all information traveling between an agency information system and any information system other than an agency information system; and

“(B) not later than 6 months after the date on which the Secretary makes available improvements to the intrusion detection and prevention capabilities pursuant to section 230(b)(2) of the Homeland Security Act of 2002 [6 U.S.C. 151(b)(2)], as added by subsection (a), whichever is later, the head of each agency shall apply and continue to utilize the capabilities to all information traveling between an agency information system and any information system other than an agency information system; and

rity Act of 2002 [6 U.S.C. 151(b)(2)], as added by subsection (a), the head of each agency shall apply and continue to utilize the improved intrusion detection and prevention capabilities.

“(2) EXCEPTION.—The requirements under paragraph (1) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

“(3) DEFINITION.—Notwithstanding section 222 [6 U.S.C. 152], in this subsection, the term ‘agency information system’ means an information system owned or operated by an agency.

“(4) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to limit an agency from applying the intrusion detection and prevention capabilities to an information system other than an agency information system under section 230(b)(1) of the Homeland Security Act of 2002 [6 U.S.C. 151(b)(1)], as added by subsection (a), at the discretion of the head of the agency or as provided in relevant policies, directives, and guidelines.”

PART D—OFFICE OF SCIENCE AND TECHNOLOGY

§ 161. Establishment of Office; Director

(a) Establishment

(1) In general

There is hereby established within the Department of Justice an Office of Science and Technology (hereinafter in this subchapter referred to as the “Office”).

(2) Authority

The Office shall be under the general authority of the Assistant Attorney General, Office of Justice Programs, and shall be established within the National Institute of Justice.

(b) Director

The Office shall be headed by a Director, who shall be an individual appointed based on approval by the Office of Personnel Management of the executive qualifications of the individual.

(Pub. L. 107–296, title II, § 231, Nov. 25, 2002, 116 Stat. 2159.)

REFERENCES IN TEXT

This subchapter, referred to in subsec. (a)(1), was in the original “this title”, meaning title II of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2145, which enacted this subchapter, amended sections 1030, 2511, 2512, 2520, 2701 to 2703, and 3125 of Title 18, Crimes and Criminal Procedure, sections 3712 and 3722 of Title 42, The Public Health and Welfare, and section 401a of Title 50, War and National Defense, and enacted provisions set out as a note under section 101 of this title and listed in a Provisions for Review, Promulgation, or Amendment of Federal Sentencing Guidelines Relating to Specific Offenses table set out under section 994 of Title 28, Judiciary and Judicial Procedure. For complete classification of title II to the Code, see Tables.

§ 162. Mission of Office; duties

(a) Mission

The mission of the Office shall be—

(1) to serve as the national focal point for work on law enforcement technology; and

(2) to carry out programs that, through the provision of equipment, training, and technical assistance, improve the safety and effectiveness of law enforcement technology and improve access to such technology by Federal, State, and local law enforcement agencies.

(b) Duties

In carrying out its mission, the Office shall have the following duties:

(1) To provide recommendations and advice to the Attorney General.

(2) To establish and maintain advisory groups (which shall be exempt from the provisions of the Federal Advisory Committee Act (5 U.S.C. App.)) to assess the law enforcement technology needs of Federal, State, and local law enforcement agencies.

(3) To establish and maintain performance standards in accordance with the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113) for, and test and evaluate law enforcement technologies that may be used by, Federal, State, and local law enforcement agencies.

(4) To establish and maintain a program to certify, validate, and mark or otherwise recognize law enforcement technology products that conform to standards established and maintained by the Office in accordance with the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113). The program may, at the discretion of the Office, allow for supplier’s declaration of conformity with such standards.

(5) To work with other entities within the Department of Justice, other Federal agencies, and the executive office of the President to establish a coordinated Federal approach on issues related to law enforcement technology.

(6) To carry out research, development, testing, evaluation, and cost-benefit analyses in fields that would improve the safety, effectiveness, and efficiency of law enforcement technologies used by Federal, State, and local law enforcement agencies, including, but not limited to—

(A) weapons capable of preventing use by unauthorized persons, including personalized guns;

(B) protective apparel;

(C) bullet-resistant and explosion-resistant glass;

(D) monitoring systems and alarm systems capable of providing precise location information;

(E) wire and wireless interoperable communication technologies;

(F) tools and techniques that facilitate investigative and forensic work, including computer forensics;

(G) equipment for particular use in counterterrorism, including devices and technologies to disable terrorist devices;

(H) guides to assist State and local law enforcement agencies;

(I) DNA identification technologies; and

(J) tools and techniques that facilitate investigations of computer crime.

(7) To administer a program of research, development, testing, and demonstration to improve the interoperability of voice and data public safety communications.

(8) To serve on the Technical Support Working Group of the Department of Defense, and on other relevant interagency panels, as requested.

(9) To develop, and disseminate to State and local law enforcement agencies, technical assistance and training materials for law enforcement personnel, including prosecutors.