tion, map, document, record, or other paper of the United States shall be deemed to be a reference to the Assistant Director for Infrastructure Security.

(b) Functions

The Assistant Director shall—

(1) direct the critical infrastructure security efforts of the Agency;

(2) carry out, at the direction of the Director, the Chemical Facilities Anti-Terrorism Standards Program established under subchapter XVI and the secure handling of ammonium nitrate program established under part J of subchapter VIII, or any successor programs;

(3) fully participate in the mechanisms required under section 652(c)(7) of this title; and

(4) carry out such other duties and powers as prescribed by the Director.

(Pub. L. 107–296, title XXII, § 2204, as added Pub. L. 115–278, § 2(a), Nov. 16, 2018, 132 Stat. 4174.)

ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION AUTHORIZED TO SERVE AS ASSISTANT DIRECTOR FOR INFRASTRUCTURE SECURITY

Pub. L. 115–278, § 2(b)(4), Nov. 16, 2018, 132 Stat. 4175, provided that: ''The individual serving as the Assistant Secretary for Infrastructure Protection on the day before the date of enactment of this Act [Nov. 16, 2018] may continue to serve as the Assistant Director for Infrastructure Security on and after such date.''

§ 655. Enhancement of Federal and non-Federal cybersecurity

In carrying out the responsibilities under section 652 of this title, the Director of Cybersecurity and Infrastructure Security 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;

(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 XXII, § 2205, formerly 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; renumbered title XXII, § 2205, and amended Pub. L. 115–278, § 2(g)(2)(I), (9)(A)(i), Nov. 16, 2018, 132 Stat. 4178, 4180.)

CODIFICATION

Section was formerly classified to section 143 of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2018—Pub. L. 115–278, § 2(g)(9)(A)(i)(I), substituted ''section 652 of this title'' for ''section 121 of this title'' and ''Director of Cybersecurity and Infrastructure Security'' for ''Under Secretary appointed under section 113(a)(1)(H) of this title'' in introductory provisions.

Par. (1)(B). Pub. L. 115–278, § 2(g)(9)(A)(i)(II), struck out ''and'' at end.

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.

§ 656. NET Guard

The Director of Cybersecurity and Infrastructure Security 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 XXII, § 2206, formerly 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; renumbered title XXII, § 2206, and amended Pub. L. 115–278, § 2(g)(2)(I), (9)(A)(ii), Nov. 16, 2018, 132 Stat. 4178, 4180.)

CODIFICATION

Section was formerly classified to section 144 of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2018—Pub. L. 115–278, § 2(g)(9)(A)(ii), substituted ''Director of Cybersecurity and Infrastructure Security'' for ''Assistant Secretary for Infrastructure Protection''.

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

§ 657. 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 na-

ture 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 XXII, § 2207, formerly title II, § 225, Nov. 25, 2002, 116 Stat. 2156; renumbered title XXII, § 2207, Pub. L. 115–278, § 2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178.)

CODIFICATION

Section was formerly classified to section 145 of this title prior to renumbering by Pub. L. 115–278.

Section is comprised of section 2207 of Pub. L. 107–296. Subsecs. (d)(1) and (e) to (j) of section 2207 of Pub. L. 107–296 amended sections 1030, 2511, 2512, 2520, 2701 to 2703, and 3125 of Title 18, Crimes and Criminal Procedure.

§ 658. 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 purpose 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;