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-