

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 non-Federal cybersecurity

In carrying out the responsibilities under section 121 of this title, the Under Secretary for Intelligence and Analysis, in cooperation with the Assistant Secretary for Infrastructure Protection¹ 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.

(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.)

AMENDMENTS

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.)

¹ So in original. Probably should be followed by a comma.

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.