and is otherwise not appropriately in the public domain.

(f) Penalties

Whoever, being an officer or employee of the United States or of any department or agency thereof, knowingly publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law, any critical infrastructure information protected from disclosure by this part coming to him in the course of this employment or official duties or by reason of any examination or investigation made by, or return, report, or record made to or filed with, such department or agency or officer or employee thereof, shall be fined under title 18, imprisoned not more than 1 year, or both, and shall be removed from office or employment.

(g) Authority to issue warnings

The Federal Government may provide advisories, alerts, and warnings to relevant companies, targeted sectors, other governmental entities, or the general public regarding potential threats to critical infrastructure as appropriate. In issuing a warning, the Federal Government shall take appropriate actions to protect from disclosure—

(1) the source of any voluntarily submitted critical infrastructure information that forms the basis for the warning; or

(2) information that is proprietary, business sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately in the public domain.

(h) Authority to delegate

The President may delegate authority to a critical infrastructure protection program, designated 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 2158 of title 50, Appendix.

(Pub. L. 107–296, title II, § 214, Nov. 25, 2002, 116 Stat. 2152.)

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.

§ 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.)

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 redissemination 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

The Secretary shall appoint a senior official in the Department 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; and

(5) 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.

(Pub. L. 107–296, title II, § 222, Nov. 25, 2002, 116 Stat. 2155.)

REFERENCES IN TEXT

The Privacy Act of 1974, referred to in pars. (2) and (5), 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.

§ 143. Enhancement of non-Federal cybersecurity

In carrying out the responsibilities under section 121 of this title, the Under Secretary for Information Analysis and Infrastructure Protection 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.)

§ 144. NET Guard

The Under Secretary for Information Analysis and 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.)

§ 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.