

(c) Intelligence component of the Department

In this section, the term “intelligence component of the Department” has the meaning given that term in section 101 of this title.

(Pub. L. 113–293, title III, §324, Dec. 19, 2014, 128 Stat. 4004.)

CODIFICATION

Section was enacted as part of the Intelligence Authorization Act for Fiscal Year 2015, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

DEFINITIONS

“Congressional intelligence committees” means the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives, see section 2 of Pub. L. 113–293, set out as a note under section 3003 of Title 50, War and National Defense.

PART B—CRITICAL INFRASTRUCTURE
INFORMATION**§ 131. Definitions**

In this part:

(1) Agency

The term “agency” has the meaning given it in section 551 of title 5.

(2) Covered Federal agency

The term “covered Federal agency” means the Department of Homeland Security.

(3) Critical infrastructure information

The term “critical infrastructure information” means information not customarily in the public domain and related to the security of critical infrastructure or protected systems—

(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

(B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or

(C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

(4) Critical infrastructure protection program

The term “critical infrastructure protection program” means any component or bureau of a covered Federal agency that has been designated by the President or any agency head to receive critical infrastructure information.

(5) Information Sharing and Analysis Organization

The term “Information Sharing and Analysis Organization” means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of—

(A) gathering and analyzing critical infrastructure information, including information related to cybersecurity risks and incidents, in order to better understand security problems and interdependencies related to critical infrastructure, including cybersecurity risks and incidents, and protected systems, so as to ensure the availability, integrity, and reliability thereof;

(B) communicating or disclosing critical infrastructure information, including cybersecurity risks and incidents, to help prevent, detect, mitigate, or recover from the effects of a¹ interference, compromise, or a² incapacitation problem related to critical infrastructure, including cybersecurity risks and incidents, or protected systems; and

(C) voluntarily disseminating critical infrastructure information, including cybersecurity risks and incidents, to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).

(6) Protected system

The term “protected system”—

(A) means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure; and

(B) includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.

(7) Voluntary**(A) In general**

The term “voluntary”, in the case of any submittal of critical infrastructure information to a covered Federal agency, means the submittal thereof in the absence of such agency’s exercise of legal authority to compel access to or submission of such information and may be accomplished by a single entity or an Information Sharing and Analysis Organization on behalf of itself or its members.

(B) Exclusions

The term “voluntary”—

(i) in the case of any action brought under the securities laws as is defined in section 78c(a)(47) of title 15—

(I) does not include information or statements contained in any documents

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

² So in original. The word “a” probably should not appear.

or materials filed with the Securities and Exchange Commission, or with Federal banking regulators, pursuant to section 78(i) of title 15; and

(II) with respect to the submittal of critical infrastructure information, does not include any disclosure or writing that when made accompanied the solicitation of an offer or a sale of securities; and

(ii) does not include information or statements submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings.

(8) Cybersecurity risk; incident

The terms “cybersecurity risk” and “incident” have the meanings given those terms in section 148 of this title.

(Pub. L. 107–296, title II, §212, Nov. 25, 2002, 116 Stat. 2150; Pub. L. 114–113, div. N, title II, §204, Dec. 18, 2015, 129 Stat. 2961.)

AMENDMENTS

2015—Par. (5)(A). Pub. L. 114–113, §204(1)(A), inserted “, including information related to cybersecurity risks and incidents,” after “critical infrastructure information” and “, including cybersecurity risks and incidents,” after “related to critical infrastructure”.

Par. (5)(B). Pub. L. 114–113, §204(1)(B), inserted “, including cybersecurity risks and incidents,” after “critical infrastructure information” and “, including cybersecurity risks and incidents,” after “related to critical infrastructure”.

Par. (5)(C). Pub. L. 114–113, §204(1)(C), inserted “, including cybersecurity risks and incidents,” after “critical infrastructure information”.

Par. (8). Pub. L. 114–113, §204(2), added par. (8).

SHORT TITLE

For short title of this part as the “Critical Infrastructure Information Act of 2002”, see section 211 of Pub. L. 107–296, set out as a note under section 101 of this title.

PROHIBITION ON NEW REGULATORY AUTHORITY

Pub. L. 114–113, div. N, title II, §210, Dec. 18, 2015, 129 Stat. 2962, provided that: “Nothing in this subtitle [subtitle A (§§201–211) of title II of div. N of Pub. L. 114–113, see Short Title of 2015 Amendment note set out under section 101 of this title] or the amendments made by this subtitle may be construed to grant the Secretary any authority to promulgate regulations or set standards relating to the cybersecurity of non-Federal entities, not including State, local, and tribal governments, that was not in effect on the day before the date of enactment of this Act [Dec. 18, 2015].”

DEFINITIONS

Pub. L. 114–113, div. N, title II, §202, Dec. 18, 2015, 129 Stat. 2956, provided that: “In this subtitle [subtitle A (§§201–211) of title II of div. N of Pub. L. 114–113, see Short Title of 2015 Amendment note set out under section 101 of this title]:

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

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

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

“(2) CYBERSECURITY RISK; INCIDENT.—The terms ‘cybersecurity risk’ and ‘incident’ have the meanings given those terms in section 227 of the Homeland Security Act of 2002 [6 U.S.C. 148], as so redesignated by section 223(a)(3) of this division.

“(3) CYBER THREAT INDICATOR; DEFENSIVE MEASURE.—The terms ‘cyber threat indicator’ and ‘defensive measure’ have the meanings given those terms in section 102 [6 U.S.C. 1501].

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

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

§ 132. Designation of critical infrastructure protection program

A critical infrastructure protection program may be designated as such by one of the following:

- (1) The President.
- (2) The Secretary of Homeland Security.

(Pub. L. 107–296, title II, §213, Nov. 25, 2002, 116 Stat. 2152.)

§ 133. Protection of voluntarily shared critical infrastructure information

(a) Protection

(1) In general

Notwithstanding any other provision of law, critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement specified in paragraph (2)—

(A) shall be exempt from disclosure under section 552 of title 5 (commonly referred to as the Freedom of Information Act);

(B) shall not be subject to any agency rules or judicial doctrine regarding ex parte communications with a decision making official;

(C) shall not, without the written consent of the person or entity submitting such information, be used directly by such agency, any other Federal, State, or local authority, or any third party, in any civil action arising under Federal or State law if such information is submitted in good faith;

(D) shall not, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or employee of the United States for purposes other than the purposes of this part, except—

(i) in furtherance of an investigation or the prosecution of a criminal act; or

(ii) when disclosure of the information would be—

(I) to either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee thereof or subcommittee of any such joint committee; or

(II) to the Comptroller General, or any authorized representative of the Comptroller General, in the course of the performance of the duties of the Government Accountability Office.¹

¹ So in original. The period probably should be a semicolon.

(E) shall not, if provided to a State or local government or government agency—

(i) be made available pursuant to any State or local law requiring disclosure of information or records;

(ii) otherwise be disclosed or distributed to any party by said State or local government or government agency without the written consent of the person or entity submitting such information; or

(iii) be used other than for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act; and

(F) does not constitute a waiver of any applicable privilege or protection provided under law, such as trade secret protection.

(2) Express statement

For purposes of paragraph (1), the term “express statement”, with respect to information or records, means—

(A) in the case of written information or records, a written marking on the information or records substantially similar to the following: “This information is voluntarily submitted to the Federal Government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002.”; or

(B) in the case of oral information, a similar written statement submitted within a reasonable period following the oral communication.

(b) Limitation

No communication of critical infrastructure information to a covered Federal agency made pursuant to this part shall be considered to be an action subject to the requirements of the Federal Advisory Committee Act.

(c) Independently obtained information

Nothing in this section shall be construed to limit or otherwise affect the ability of a State, local, or Federal Government entity, agency, or authority, or any third party, under applicable law, to obtain critical infrastructure information in a manner not covered by subsection (a), including any information lawfully and properly disclosed generally or broadly to the public and to use such information in any manner permitted by law. 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.

(d) Treatment of voluntary submittal of information

The voluntary submittal to the Government of information or records that are protected from disclosure by this part shall not be construed to constitute compliance with any requirement to submit such information to a Federal agency under any other provision of law.

(e) Procedures

(1) In general

The Secretary of the Department of Homeland Security shall, in consultation with appropriate representatives of the National Se-

curity Council and the Office of Science and Technology Policy, establish uniform procedures for the receipt, care, and storage by Federal agencies of critical infrastructure information that is voluntarily submitted to the Government. The procedures shall be established not later than 90 days after November 25, 2002.

(2) Elements

The procedures established under paragraph (1) shall include mechanisms regarding—

(A) the acknowledgement of receipt by Federal agencies of critical infrastructure information that is voluntarily submitted to the Government;

(B) the maintenance of the identification of such information as voluntarily submitted to the Government for purposes of and subject to the provisions of this part;

(C) the care and storage of such information; and

(D) the protection and maintenance of the confidentiality of such information so as to permit the sharing of such information within the Federal Government and with State and local governments, and the issuance of notices and warnings related to the protection of critical infrastructure and protected systems, in such manner as to protect from public disclosure the identity of the submitting person or entity, or information that is proprietary, business sensitive, relates specifically to the submitting person or entity, 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, des-

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