

(d) Mission promotion

The Director may use appropriated amounts to purchase promotional and recognition items and marketing and advertising services to publicize and promote the mission and services of the Agency, support the activities of the Agency, and to recruit and retain Agency personnel. (Pub. L. 107-296, title XXII, § 2217, as added Pub. L. 116-283, div. A, title XVII, § 1719(c), Jan. 1, 2021, 134 Stat. 4106.)

PART B—CRITICAL INFRASTRUCTURE
INFORMATION

Editorial Notes

CODIFICATION

Subtitle B of title XXII of Pub. L. 107-296, comprising this part, was originally added as subtitle B of title II of Pub. L. 107-296, and was classified to part B (§131 et seq.) of subchapter II of this chapter. Subtitle B of title II of Pub. L. 107-296 was subsequently redesignated subtitle B of title XXII of Pub. L. 107-296 by Pub. L. 115-278, §2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178, and transferred to this part.

§ 671. 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—

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

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

(I) does not include information or statements contained in any documents 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 659 of this title.

(Pub. L. 107–296, title XXII, § 2222, formerly title II, § 212, Nov. 25, 2002, 116 Stat. 2150; Pub. L. 114–113, div. N, title II, § 204, Dec. 18, 2015, 129 Stat. 2961; renumbered title XXII, § 2222, and amended Pub. L. 115–278, § 2(g)(2)(H), (9)(B)(i), Nov. 16, 2018, 132 Stat. 4178, 4181.)

Editorial Notes

CODIFICATION

Section was formerly classified to section 131 of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2018—Par. (8). Pub. L. 115–278, § 2(g)(9)(B)(i), substituted “section 659 of this title” for “section 148 of this title”.

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).

Statutory Notes and Related Subsidiaries

SHORT TITLE

For short title of this part as the “Critical Infrastructure Information Act of 2002”, see section 2221 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, as amended by Pub. L. 115–278, § 2(h)(1)(A), Nov. 16, 2018, 132 Stat. 4181, 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 2209 of the Homeland Security Act of 2002 [6 U.S.C. 659].

“(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.”

§ 672. 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 XXII, § 2223, formerly title II, § 213, Nov. 25, 2002, 116 Stat. 2152; renumbered title XXII, § 2223, Pub. L. 115–278, § 2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178.)

Editorial Notes

CODIFICATION

Section was formerly classified to section 132 of this title prior to renumbering by Pub. L. 115–278.

§ 673. 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;