

“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] [see now 6 U.S.C. 650].

“(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;

(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.<sup>1</sup>

(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.

<sup>1</sup> So in original. The period probably should be a semicolon.

**(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 chapter 10 of title 5.

**(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 Security 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, designated under section 672 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 XXII, §2224, formerly 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; renumbered title XXII, §2224, and amended Pub. L. 115-278, §2(g)(2)(H), (9)(B)(ii), Nov. 16, 2018, 132 Stat. 4178, 4181; Pub. L. 117-286, §4(a)(18), Dec. 27, 2022, 136 Stat. 4307.)

**Editorial Notes****REFERENCES IN TEXT**

The Critical Infrastructure Information Act of 2002, referred to in subsec. (a)(2)(A), is subtitle B (§2221 et

seq.) of title XXII 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.

#### CODIFICATION

Section was formerly classified to section 133 of this title prior to renumbering by Pub. L. 115–278.

#### AMENDMENTS

2022—Subsec. (b). Pub. L. 117–286 substituted “chapter 10 of title 5.” for “the Federal Advisory Committee Act.”

2018—Subsec. (h). Pub. L. 115–278, § 2(g)(9)(B)(ii), substituted “section 672 of this title” for “section 132 of this title”.

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”.

#### Statutory Notes and Related Subsidiaries

##### 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.

#### § 674. 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 XXII, § 2225, formerly title II, § 215, Nov. 25, 2002, 116 Stat. 2155; renumbered title XXII, § 2225, Pub. L. 115–278, § 2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178.)

#### Editorial Notes

##### 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.

#### CODIFICATION

Section was formerly classified to section 134 of this title prior to renumbering by Pub. L. 115–278.

#### PART C—DECLARATION OF A SIGNIFICANT INCIDENT

#### § 677. Sense of Congress

It is the sense of Congress that—

(1) the purpose of this part is to authorize the Secretary to declare that a significant incident has occurred and to establish the authorities that are provided under the declaration to respond to and recover from the significant incident; and

(2) the authorities established under this part are intended to enable the Secretary to provide voluntary assistance to non-Federal entities impacted by a significant incident.

(Pub. L. 107–296, title XXII, § 2231, as added Pub. L. 117–58, div. G, title VI, § 70602(a), Nov. 15, 2021, 135 Stat. 1267.)

#### § 677a. Definitions

For the purposes of this part:

##### (1) Asset response activity

The term “asset response activity” means an activity to support an entity impacted by an incident with the response to, remediation of, or recovery from, the incident, including—

(A) furnishing technical and advisory assistance to the entity to protect the assets of the entity, mitigate vulnerabilities, and reduce the related impacts;

(B) assessing potential risks to the critical infrastructure sector or geographic region impacted by the incident, including potential cascading effects of the incident on other critical infrastructure sectors or geographic regions;

(C) developing courses of action to mitigate the risks assessed under subparagraph (B);

(D) facilitating information sharing and operational coordination with entities performing threat response activities; and

(E) providing guidance on how best to use Federal resources and capabilities in a timely, effective manner to speed recovery from the incident.

##### (2) Declaration

The term “declaration” means a declaration of the Secretary under section 677b(a)(1) of this title.

##### (3) Director

The term “Director” means the Director of the Cybersecurity and Infrastructure Security Agency.

##### (4) Federal agency

The term “Federal agency” has the meaning given the term “agency” in section 3502 of title 44.

##### (5) Fund

The term “Fund” means the Cyber Response and Recovery Fund established under section 677c(a) of this title.

##### (6) Incident

The term “incident” has the meaning given the term in section 3552 of title 44.

##### (7) Renewal

The term “renewal” means a renewal of a declaration under section 677b(d) of this title.

##### (8) Significant incident

The term “significant incident”—

(A) means an incident or a group of related incidents that results, or is likely to result, in demonstrable harm to—

(i) the national security interests, foreign relations, or economy of the United States; or

(ii) the public confidence, civil liberties, or public health and safety of the people of the United States; and

(B) does not include an incident or a portion of a group of related incidents that occurs on—

(i) a national security system (as defined in section 3552 of title 44); or