

## 6 USCS § 673

Current through Public Law 118-62, approved May 13, 2024.

*United States Code Service* > **TITLE 6. DOMESTIC SECURITY (§§ 101 — 1534)** > **CHAPTER 1. HOMELAND SECURITY ORGANIZATION (§§ 101 — 681g)** > **CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (§§ 650 — 681g)** > **CRITICAL INFRASTRUCTURE INFORMATION (§§ 671 — 674)**

### **§ 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, United States Code (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 subtitle [6 USCS §§ 131 et seq.], 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 General Accounting Office [Government Accountability Office].[:]

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

## § 673. Protection of voluntarily shared critical infrastructure information

- (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 subtitle [6 USCS §§ 131 et seq.] shall be considered to be an action subject to the requirements of chapter 10 of title 5, United States Code [5 USCS §§ 1001 et seq.].

**(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, United States Code.

**(d) Treatment of voluntary submittal of information.** The voluntary submittal to the Government of information or records that are protected from disclosure by this subtitle [6 USCS §§ 131 et seq.] 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 the date of the enactment of this subtitle [enacted Nov. 25, 2002].

(2) **Elements.** The procedures established under paragraph (1) shall include mechanisms regarding—

## § 673. Protection of voluntarily shared critical infrastructure information

- (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 subtitle [6 USCS §§ 131 et seq.];
- (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 subtitle [6 USCS §§ 131 et seq.] 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 of the United States Code, 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 2223 [6 USCS § 672], 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 708 of the Defense Production Act of 1950 (50 U.S.C. App. 2158 [50 USCS § 4558]).

## History

---

### HISTORY:

Nov. 25, 2002, P. L. 107-296, Title XXII [II], Subtitle B, § 2224 [214], 116 Stat. 2152; Nov. 27, 2012, P. L. 112-199, Title I, § 111, 126 Stat. 1472; Nov. 16, 2018, P.L. 115-278, § 2(g)(2)(H), (9)(B)(ii), 132 Stat. 4178, 4181; Dec. 27, 2022, P.L. 117-286, § 4(a)(18), 136 Stat. 4307.

§ 673. Protection of voluntarily shared critical infrastructure information

United States Code Service  
Copyright © 2024 All rights reserved.

---

End of Document