

[72 FR 65420, Nov. 20, 2007]

## PART 29—PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

Sec.

- 29.1 Purpose and scope.
- 29.2 Definitions.
- 29.3 Effect of provisions.
- 29.4 Protected Critical Infrastructure Information Program administration.
- 29.5 Requirements for protection.
- 29.6 Acknowledgment of receipt, validation, and marking.
- 29.7 Safeguarding of Protected Critical Infrastructure Information.
- 29.8 Disclosure of Protected Critical Infrastructure Information.
- 29.9 Investigation and reporting of violation of PCII procedures.

AUTHORITY: Pub. L. 107–296, 116 Stat. 2135 (6 U.S.C. 1 *et seq.*); 5 U.S.C. 301.

SOURCE: 71 FR 52271, Sept. 1, 2006, unless otherwise noted.

### § 29.1 Purpose and scope.

(a) *Purpose of this Part.* This part implements sections 211 through 215 of the Homeland Security Act of 2002 (HSA) through the establishment of uniform procedures for the receipt, care, and storage of Critical Infrastructure Information (CII) voluntarily submitted to the Department of Homeland Security (DHS). Title II, Subtitle B, of the Homeland Security Act is referred to herein as the Critical Infrastructure Information Act of 2002 (CII Act). Consistent with the statutory mission of DHS to prevent terrorist attacks within the United States and reduce the vulnerability of the United States to terrorism, DHS will encourage the voluntary submission of CII by safeguarding and protecting that information from unauthorized disclosure and by ensuring that such information is, as necessary, securely shared with State and local government pursuant to section 214(a) through (g) of the CII Act. As required by the CII Act, these rules establish procedures regarding:

- (1) The acknowledgement of receipt by DHS of voluntarily submitted CII;
- (2) The receipt, validation, handling, storage, proper marking and use of information as PCII;
- (3) The safeguarding and maintenance of the confidentiality of such information, appropriate sharing of such

information with State and local governments pursuant to section 214(a) through (g) of the HSA.

(4) The issuance of advisories, notices and warnings related to the protection of critical infrastructure or protected systems in such a manner as to protect from unauthorized disclosure the source of critical infrastructure information that forms the basis of the warning, and any information that is proprietary or business sensitive, might be used to identify the submitting person or entity, or is otherwise not appropriately in the public domain.

(b) *Scope.* The regulations in this part apply to all persons and entities that are authorized to handle, use, or store PCII or that otherwise accept receipt of PCII.

### § 29.2 Definitions.

For purposes of this part:

(a) *Critical Infrastructure* has the meaning stated in section 2 of the Homeland Security Act of 2002 (referencing the term used in section 1016(e) of Public Law 107–56 (42 U.S.C. 5195c(e)).

(b) *Critical Infrastructure Information*, or *CII*, has the same meaning as established in section 212 of the CII Act of 2002 and means information not customarily in the public domain and related to the security of critical infrastructure or protected systems, including documents, records or other information concerning:

(1) 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, local, or tribal law, harms interstate commerce of the United States, or threatens public health or safety;

(2) The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or

## § 29.2

## 6 CFR Ch. I (1–1–11 Edition)

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

(3) 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.

(c) *Information Sharing and Analysis Organization*, or *ISAO*, has the same meaning as is established in section 212 of the CII Act of 2002 and means any formal or informal entity or collaboration created or employed by public or private sector organizations for purposes of:

(1) Gathering and analyzing CII in order to better understand security problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability thereof;

(2) Communicating or disclosing CII to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or an incapacitation problem related to critical infrastructure or protected systems; and

(3) Voluntarily disseminating CII to its members, Federal, State, and local governments, or any other entities that may be of assistance in carrying out the purposes specified in paragraphs (c)(1) and (2) of this section.

(d) *In the public domain* means information lawfully, properly and regularly disclosed generally or broadly to the public. Information regarding system, facility or operational security is not “in the public domain.” Information submitted with CII that is proprietary or business sensitive, or which might be used to identify a submitting person or entity will not be considered “in the public domain.” Information may be “business sensitive” for this purpose whether or not it is commercial in nature, and even if its release could not demonstrably cause substantial harm to the competitive position of the submitting person or entity.

(e) *Local government* has the same meaning as is established in section 2 of the Homeland Security Act of 2002 and means:

(1) A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a non-profit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government;

(2) An Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and

(3) A rural community, unincorporated town or village, or other public entity.

(f) *Program Manager’s Designee* means a Federal employee outside of the PCII Program Office, whether employed by DHS or another Federal agency, to whom certain functions of the PCII Program Office are delegated by the Program Manager, as determined on a case-by-case basis.

(g) *Protected Critical Infrastructure Information*, or *PCII*, means validated CII, including information covered by 6 CFR 29.6(b) and (f), including the identity of the submitting person or entity and any person or entity on whose behalf the submitting person or entity submits the CII, that is voluntarily submitted, directly or indirectly, to DHS, for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other appropriate purpose, and any information, statements, compilations or other materials reasonably necessary to explain the CII, put the CII in context, describe the importance or use of the CII, when accompanied by an express statement as described in 6 CFR 29.5.

(h) *Protected Critical Infrastructure Information Program*, or *PCII Program*, means the program implementing the CII Act, including the maintenance, management, and review of the information provided in furtherance of the protections provided by the CII Act.

(i) *Protected system* has the meaning set forth in section 212(6) of the CII

Act, and 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 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.

(j) *Purposes of the CII Act* has the meaning set forth in section 214(a)(1) of the CII Act and includes the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose.

(k) *Regulatory proceeding*, as used in section 212(7) of the CII Act and these rules, means administrative proceedings in which DHS is the adjudicating entity, and does not include any form or type of regulatory proceeding or other matter outside of DHS.

(l) *State* has the same meaning set forth in section 2 of the Homeland Security Act of 2002 and means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States.

(m) *Submission* as referenced in these procedures means any transmittal, either directly or indirectly, of CII to the DHS PCII Program Manager or the PCII Program Manager's designee, as set forth herein.

(n) *Submitted in good faith* means any submission of information that could reasonably be defined as CII or PCII under this section. Upon validation of a submission as PCII, DHS has conclusively established the good faith of the submission. Any information qualifying as PCII by virtue of a categorical inclusion identified by the Program Manager pursuant to section 214 of the CII Act and this part is submitted in good faith.

(o) *Voluntary* or *voluntarily*, when used in reference to any submission of CII, means the submittal thereof in the

absence of an exercise of legal authority by DHS to compel access to or submission of such information. Voluntary submission of CII may be accomplished by (*i.e.*, come from) a single state or local governmental entity; private entity or person; or by an ISAO acting on behalf of its members or otherwise. There are two exclusions from this definition. In the case of any action brought under the securities laws—as is defined in section 3(a)(47) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(47))—the term “voluntary” or “voluntarily” does not include information or statements contained in any documents or materials filed, pursuant to section 12(i) of the Securities Exchange Act of 1934 (15 U.S.C. 781(i)), with the U.S. Securities and Exchange Commission or with Federal banking regulators or a writing that accompanied the solicitation of an offer or a sale of securities. Information or statements previously submitted to DHS in the course of a regulatory proceeding or a licensing or permitting determination are not “voluntarily submitted.” In addition, the submission of information to DHS for purposes of seeking a Federal preference or benefit, including CII submitted to support an application for a DHS grant to secure critical infrastructure will be considered a voluntary submission of information. Applications for SAFETY Act Designation or Certification under 6 CFR part 25 will also be considered a voluntary submission.

(p) The term *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* in section 214(a)(1)(C) of the CII Act means any use in any proceeding other than a criminal prosecution before any court of the United States or of a State or otherwise, of any PCII, or any drafts or copies of PCII retained by the submitter, including the opinions, evaluations, analyses and conclusions prepared and submitted as CII, as evidence at trial or in any pretrial or other discovery, notwithstanding whether the United States, its agencies, officers, or employees is or are a party to such proceeding.