

§ 29.7

6 CFR Ch. I (1–15 Edition)

(C) Advise the submitting person or entity that the submission can be withdrawn at any time before a final determination is made;

(D) Notify the submitting person or entity that until a final determination is made the submission will be treated as PCII;

(E) Notify the submitting person or entity that any response to the notification must be received by the PCII Program Office no later than thirty calendar days after the date of the notification; and

(F) Request the submitting person or entity to state whether, in the event the PCII Program Office makes a final determination that any such information is not PCII, the submitting person or entity prefers that the information be maintained without the protections of the CII Act or returned to the submitter or destroyed. If a request for withdrawal is made, all such information shall be returned to the submitting person or entity.

(i) If the information submitted has not been withdrawn by the submitting person or entity, and the PCII Program Office, after following the procedures set forth in paragraph (e)(2)(i) of this section, makes a final determination that the information is not PCII, the PCII Program Office, in accordance with the submitting person or entity's written preference, shall, within thirty calendar days of making a final determination, return the information to the submitter. If return to the submitter is impractical, the PCII Program Office shall destroy the information within 30 days. This process is consistent with the appropriate National Archives and Records Administration-approved records disposition schedule. If the submitting person or entity cannot be notified or the submitting person or entity's response is not received within thirty calendar days of the date of the notification as provided in paragraph (e)(2)(i) of this section, the PCII Program Office shall make the initial determination final and return the information to the submitter.

(f) *Categorical Inclusions of Certain Types of Infrastructure as PCII.* The PCII Program Manager has discretion to declare certain subject matter or

types of information categorically protected as PCII and to set procedures for receipt and processing of such information. Information within a categorical inclusion will be considered validated upon receipt by the Program Office or any of the Program Manager's designees without further review, provided that the submitter provides the express statement required by section 214(a)(1). Designees shall provide to the Program Manager information submitted under a categorical inclusion.

(g) *Changing the status of PCII to non-PCII.* Once information is validated, only the PCII Program Office may change the status of PCII to that of non-PCII and remove its PCII markings. Status changes may only take place when the submitting person or entity requests in writing that the information no longer be protected under the CII Act; or when the PCII Program Office determines that the information was, at the time of the submission, customarily in the public domain. Upon making an initial determination that a change in status may be warranted, but prior to a final determination, the PCII Program Office, using the procedures in paragraph (e)(2) of this section, shall inform the submitting person or entity of the initial determination of a change in status. Notice of the final change in status of PCII shall be provided to all recipients of that PCII under 6 CFR 29.8.

§ 29.7 Safeguarding of Protected Critical Infrastructure Information.

(a) *Safeguarding.* All persons granted access to PCII are responsible for safeguarding such information in their possession or control. PCII shall be protected at all times by appropriate storage and handling. Each person who works with PCII is personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to it.

(b) *Background Checks on Persons with Access to PCII.* For those who require access to PCII, DHS will, to the extent practicable and consistent with the purposes of the Act, undertake appropriate background checks to ensure that individuals with access to PCII do not pose a threat to national security.

These checks may also be waived in exigent circumstances.

(c) *Use and Storage.* When PCII is in the physical possession of a person, reasonable steps shall be taken, in accordance with procedures prescribed by the PCII Program Manager, to minimize the risk of access to PCII by unauthorized persons. When PCII is not in the physical possession of a person, it shall be stored in a secure environment.

(d) *Reproduction.* Pursuant to procedures prescribed by the PCII Program Manager, a document or other material containing PCII may be reproduced to the extent necessary consistent with the need to carry out official duties, provided that the reproduced documents or material are marked and protected in the same manner as the original documents or material.

(e) *Disposal of information.* Documents and material containing PCII may be disposed of by any method that prevents unauthorized retrieval, such as shredding or incineration.

(f) *Transmission of information.* PCII shall be transmitted only by secure means of delivery as determined by the PCII Program Manager, and in conformance with appropriate federal standards.

(g) *Automated Information Systems.* The PCII Program Manager shall establish security requirements designed to protect information to the maximum extent practicable, and consistent with the Act, for Automated Information Systems that contain PCII. Such security requirements will be in conformance with the information technology security requirements in the Federal Information Security Management Act and the Office of Management and Budget's implementing policies.

§ 29.8 Disclosure of Protected Critical Infrastructure Information.

(a) *Authorization of access.* The Under Secretary for Preparedness, the Assistant Secretary for Infrastructure Protection, or either's designee may choose to provide or authorize access to PCII under one or more of the subsections below when it is determined that this access supports a lawful and authorized government purpose as enu-

merated in the CII Act or other law, regulation, or legal authority.

(b) *Federal, State and Local government sharing.* The PCII Program Manager or the PCII Program Manager's designees may provide PCII to an employee of the Federal government, provided, subject to subsection (f) of this section, that such information is shared for purposes of securing the critical infrastructure or protected systems, analysis, warning, interdependency study, recovery, reconstitution, or for another appropriate purpose including, without limitation, the identification, analysis, prevention, preemption, and/or disruption of terrorist threats to the homeland. PCII may not be used, directly or indirectly, for any collateral regulatory purpose. PCII may be provided to a State or local government entity for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act. The provision of PCII to a State or local government entity will normally be made only pursuant to an arrangement with the PCII Program Manager providing for compliance with the requirements of paragraph (d) of this section and acknowledging the understanding and responsibilities of the recipient. State and local governments receiving such information will acknowledge in such arrangements the primacy of PCII protections under the CII Act; agree to assert all available legal defenses to disclosure of PCII under State, or local public disclosure laws, statutes or ordinances; and will agree to treat breaches of the agreements by their employees or contractors as matters subject to the criminal code or to the applicable employee code of conduct for the jurisdiction.

(c) *Disclosure of information to Federal, State and local government contractors.* Disclosure of PCII to Federal, State, and local contractors may be made when necessary for an appropriate purpose under the CII Act, and only after the PCII Program Manager or a PCII Officer certifies that the contractor is performing services in support of the purposes of the CII Act. The contractor's employees who will be handling PCII must sign individual nondisclosure agreements in a form prescribed