

PCII is used only for appropriate purposes.

§ 29.4 Protected Critical Infrastructure Information Program administration.

(a) *Preparedness Directorate Program Management.* The Secretary of Homeland Security hereby designates the Under Secretary for Preparedness as the senior DHS official responsible for the direction and administration of the PCII Program. He shall administer this program through the Assistant Secretary for Infrastructure Protection.

(b) *Appointment of a PCII Program Manager.* The Under Secretary for Preparedness shall:

(1) Appoint a PCII Program Manager serving under the Assistant Secretary for Infrastructure Protection who is responsible for the administration of the PCII Program;

(2) Commit resources necessary for the effective implementation of the PCII Program;

(3) Ensure that sufficient personnel, including such detailees or assignees from other Federal national security, homeland security, or law enforcement entities as the Under Secretary deems appropriate, are assigned to the PCII Program to facilitate secure information sharing with appropriate authorities.

(4) Promulgate implementing directives and prepare training materials as appropriate for the proper treatment of PCII.

(c) *Appointment of PCII Officers.* The PCII Program Manager shall establish procedures to ensure that each DHS component and each Federal, State, or local entity that works with PCII appoint one or more employees to serve as a PCII Officer in order to carry out the responsibilities stated in paragraph (d) of this section. Persons appointed to serve as PCII Officers shall be fully familiar with these procedures.

(d) *Responsibilities of PCII Officers.* PCII Officers shall:

(1) Oversee the handling, use, and storage of PCII;

(2) Ensure the secure sharing of PCII with appropriate authorities and individuals, as set forth in 6 CFR 29.1(a), and paragraph (b)(3) of this section;

(3) Establish and maintain an ongoing self-inspection program, to include periodic review and assessment of the compliance with handling, use, and storage of PCII;

(4) Establish additional procedures, measures and penalties as necessary to prevent unauthorized access to PCII; and

(5) Ensure prompt and appropriate coordination with the PCII Program Manager regarding any request, challenge, or complaint arising out of the implementation of these regulations.

(e) *Protected Critical Infrastructure Information Management System (PCIIMS).* The PCII Program Manager shall develop, for use by the PCII Program Manager and the PCII Manager's designees, an electronic database, to be known as the "Protected Critical Infrastructure Information Management System" (PCIIMS), to record the receipt, acknowledgement, validation, storage, dissemination, and destruction of PCII. This compilation of PCII shall be safeguarded and protected in accordance with the provisions of the CII Act. The PCII Program Manager may require the completion of appropriate background investigations of an individual before granting that individual access to any PCII.

§ 29.5 Requirements for protection.

(a) CII shall receive the protections of section 214 of the CII Act when:

(1) Such information is voluntarily submitted, directly or indirectly, to the PCII Program Manager or the PCII Program Manager's designee;

(2) The information is submitted for protected use regarding the security of critical infrastructure or protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other appropriate purposes including, without limitation, for the identification, analysis, prevention, preemption, disruption, defense against and/or mitigation of terrorist threats to the homeland;

(3) The information is labeled with an express statement as follows:

(i) In the case of documentary submissions, written marking on the information or records substantially similar to the following: "This information is voluntarily submitted to the