

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

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

(d) *Responsibilities of Protected CII Officers.* Protected CII Officers shall:

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

(2) Ensure the expeditious and secure sharing of Protected CII with appropriate authorities, as set forth in § 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 entity's handling, use, and storage of Protected CII;

(4) Establish additional procedures as necessary to prevent unauthorized access to Protected CII; and

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

(e) *Protected Critical Infrastructure Information Management System (PCIIMS).* The Protected CII Program Manager or the Protected CII Program Manager's designees shall develop and use 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 Protected CII. This compilation of Protected CII shall be safeguarded and protected in accordance with the provisions of the CII Act of 2002.

#### § 29.5 Requirements for protection.

(a) CII shall receive the protections of section 214 of the CII Act of 2002 only when:

(1) Such information is voluntarily submitted to the Protected CII Program Manager or the Protected CII Program Manager's designees;

(2) The information is submitted for use by DHS for the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purposes including, without limitation, the identification, analysis, prevention, preemption, and/or disruption of terrorist threats to our homeland, as evidenced below;

(3) The information is accompanied by an express statement as follows:

(i) In the case of written information or records, through 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

(ii) In the case of oral information, within fifteen calendar days of the oral submission, through a written statement comparable to the one specified above, and a certification as specified below, accompanied by a written or otherwise tangible version of the oral information initially provided; and

(4) The submitted information additionally is accompanied by a statement, signed by the submitting entity, certifying essentially to the following on behalf of the named entity:

(i) The submitter is voluntarily providing the information for the purposes of the CII Act of 2002;

(ii) The information being submitted is not being submitted in lieu of independent compliance with a Federal legal requirement;

(iii) The information is or is not required to be submitted to a Federal agency. If the information is required to be submitted to a Federal agency, the submitter shall identify the Federal agency requiring submission and the legal authority that mandates the submission; and

(iv) The information is of a type not customarily in the public domain.

(b) Information that is not submitted to the Protected CII Program Manager or the Protected CII Program Manager's designees will not qualify for protection under the CII Act of 2002. Any DHS component other than the IAIP Directorate that receives information with a request for protection under the CII Act of 2002, shall immediately forward the information to the Protected CII Program Manager. Only the Protected CII Program Manager or the Protected CII Program Manager's designees are authorized to acknowledge receipt and validate Protected CII pursuant to § 29.6(a).

(c) Federal agencies and DHS components other than the IAIP Directorate shall maintain information as protected by the provisions of the CII Act of 2002 when that information is provided to the agency or component by the Protected CII Program Manager or the Protected CII Program Manager's designees and is marked as required in § 29.6(c).

(d) All submissions seeking Protected CII status shall be regarded as submitted with the presumption of good faith on the part of the submitter.

(e) Submissions must affirm the understanding of the submitter that any false representations on such submissions may constitute a violation of 18 U.S.C. 1001 and are punishable by fine and imprisonment.

**§ 29.6 Acknowledgment of receipt, validation, and marking.**

(a) *Authorized officials.* Only the Protected CII Program Manager or the Protected CII Program Manager's designees are authorized to acknowledge receipt of and validate information as Protected CII.

(b) *Presumption of protection.* All information submitted in accordance with the procedures set forth herein will be presumed to be and will be treated as Protected CII from the time the information is received by DHS, either through the DHS component or the Protected CII Program Manager or the Protected CII Program Manager's designees. The information shall remain protected unless and until the Protected CII Program Manager or the

Protected CII Program Manager's designees render a final decision that the information is not Protected CII.

(c) *Marking of information.* In addition to markings made pursuant to § 29.5(a) by submitters of CII requesting review, all Protected CII shall be clearly identified through markings made by the Protected CII Program Manager or the Protected CII Program Manager's designees. The Protected CII Program Manager or the Protected CII Program Manager's designees shall mark Protected CII materials as follows: "This document contains Protected CII. In accordance with the provisions of 6 CFR part 29, it is exempt from release under the Freedom of Information Act (5 U.S.C. 552(b)(3)). Unauthorized release may result in civil penalty or other action. It is to be safeguarded and disseminated in accordance with Protected CII Program requirements."

(d) *Acknowledgement of receipt of information.* The Protected CII Program Manager or the Protected CII Program Manager's designees shall acknowledge receipt of information submitted as CII and accompanied by an express statement and certification, and in so doing shall:

(1) Contact the submitter, within thirty calendar days of receipt, by the means of delivery prescribed in procedures developed by the Protected CII Program Manager or the Protected CII Program Manager. In the case of oral submissions, receipt will be acknowledged in writing within thirty calendar days after receipt by the Protected CII Program Manager or the Protected CII Program Manager's designees of a written statement, certification, and documentation of the oral submission, as referenced in § 29.5(a)(3)(ii);

(2) Maintain a database including date of receipt, name of submitter, description of information, manner of acknowledgment, tracking number, and validation status; and

(3) Provide the submitter with a unique tracking number that will accompany the information from the time it is received by the Protected CII Program Manager or the Protected CII Program Manager's designees.

(e) *Validation of information.* (1) The Protected CII Program Manager or the