

oral submission, through a written statement similar to the one above accompanied by a written or otherwise tangible version of the oral information initially provided.

(c) Information that is not submitted to the CII Program Manager, either directly by the submitter or indirectly through another Federal agency by request of the submitter, will not qualify for protection under the CII Act of 2002. Any Federal agency or DHS component, other than the IAIP Directorate, that receives information with a request for protection under the CII Act of 2002 shall forward the information to the CII Program Manager. Only the CII Program Manager, or the Program Manager's designee, is authorized to acknowledge and validate the receipt of Protected CII.

(d)(1) Federal agencies, or DHS components other than the IAIP Directorate, shall maintain information as protected by the provisions of the CII Act of 2002 only:

(i) When that information is provided to the agency or component by the CII Program Manager, or his designee, and is marked "Protected CII"; or

(ii) When the information is provided to the agency or component by the submitter pursuant to paragraph (b) of this section, that information is forwarded to the CII Program Manager pursuant to paragraph (c) of this section, and the CII Program Manager acknowledges and validates the information as "Protected CII" and authorizes the agency or component to mark the information as "Protected CII".

(2) The Federal agency or DHS component forwarding the information to the CII Program Manager may not disseminate, distribute, or make public the information until the CII Program Manager has notified the agency or component that the Program Manager has acknowledged and validated the information.

§ 29.6 Acknowledgment, validation, and marking of receipt.

(a) *Authorized official.* Only the CII Program Manager, or the Program Manager's designee, is authorized to acknowledge and validate the receipt of information as Protected CII.

(b) *Presumption of Protection.* All information submitted in accordance with the procedures set forth herein will be presumed to be treated as Protected CII from the time the information is received by a Federal agency or DHS component. The information shall remain protected unless and until the CII Program Manager renders a final decision that the information is not Protected CII.

(c) *Marking of information.* In addition to markings made by submitters of CII pursuant to § 29.5(b), all Protected CII shall be clearly identified through markings made by the CII Program Manager. The CII Program Manager shall mark CII materials as follows: "Protected Critical Infrastructure Information."

(d) *Acknowledgement of receipt of information.* The CII Program Manager, or the Program Manager's designee, shall acknowledge receipt of information submitted as Protected CII, and in so doing shall:

(1) Contact the submitter, by the means specified in § 29.7(e), within thirty (30) days of receipt;

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

(1) At a minimum, provide the submitter with a unique tracking number whenever the information is provided to the CII Program Manager electronically by submission through an internet-enabled DHS on-line incident reporting form.

(e) *Validation of information.* (1) The CII Program Manager shall be responsible for reviewing all submissions that request protection under the CII Act of 2002. The Program Manager shall review the submitted information to validate the satisfaction of the definition of CII as established by law. In making this initial validation determination, the Program Manager shall give deference to the submitter's expectation that the information qualifies for protection. However, if the Program Manager makes an initial determination that some or all of the information submitted does not meet the requirements for protection under the CII Act of 2002, the CII Program Manager shall:

(i) Notify the submitter of the initial determination that the information is not considered to be Protected CII. This notification also shall:

(A) Request that the submitter further explain the nature of the information and the submitter's basis for believing the information qualifies for protection under the CII Act of 2002;

(B) Advise the submitter that the CII Program Manager will review any further information provided before rendering a final determination;

(C) Notify the submitter that any response to the notification must be received by the CII Program Manager no later than thirty (30) days after the date of the notification; and

(D) Request the submitter to state whether, in the event the CII Program Manager makes a final determination

that any such information is not Protected CII, the submitter prefers that the information be maintained without the protections of the CII Act of 2002 or be disposed of in accordance with the Federal Records Act.

(ii) If the CII Program Manager makes a final determination that the information is not Protected CII, the Program Manager, per the submitter's stated preference, shall either maintain the information without the protections of the CII Act of 2002 or dispose of it in accordance with the Federal Records Act. If the submitter, however, cannot be notified or the submitter's response is not received within thirty (30) days after the submitter received the notification, the Program Manager shall destroy the information in accordance with the Federal Records Act unless the Program Manager determines that there is a need to retain it for law enforcement and/or national security reasons.

(2) [Reserved]

(f) In the event the CII Program Manager determines that any information is not submitted in good faith accordance with the CII Act of 2002 and these procedures, the Program Manager is not required to notify the submitter that the information does not qualify as Protected CII. This is the only exception to the notice requirement of these procedures.

(g) *Changing the status of CII to Non-CII.* Only the CII Program Manager or the Program Manager's designee may change the status of Protected CII to non-Protected CII and remove its Protected CII markings.

§ 29.7 Safeguarding of protected Critical Infrastructure Information.

(a) All persons granted access to Protected CII are responsible for safeguarding all such information in their possession or control. Protected CII shall be protected at all times either by appropriate storage or having it under the personal observation and control of a person authorized by the CII Officer to receive it. Each person who works with Protected CII is personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to it.

(b) *Use and storage.* During working hours, reasonable steps shall be taken to minimize the risk of access to Protected CII by unauthorized personnel. After working hours, Protected CII shall be stored in a secure container, such as a locked desk or file cabinet, or in a facility where Government or Government-contract security is provided.

(c) *Reproduction.* A document or material containing Protected CII may