

CII to DHS, means submitted in the absence of DHS's exercise of legal authority to compel access to or submission of such information; such submission may be accomplished by (*i.e.* come from) a single entity or an ISAO on behalf of itself or its members. The term does not include information or statements submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings. 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” 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. 78l(i)) with the Securities and Exchange Commission or with Federal banking regulators; and with respect to the submission of CII, it does not include any disclosure or writing that when made accompanied the solicitation of an offer or a sale of securities.

§ 29.3 Effect of provisions.

(a) *Freedom of Information Act access and mandatory submissions of information.* The CII Act of 2002 and these procedures do not apply to or affect any requirement pertaining to information that must be submitted to a Federal agency or pertaining to the obligation of any Federal agency to disclose such information under the Freedom of Information Act. Similarly, the CII Act of 2002 and these procedures do not apply to any information that is submitted to a Federal agency pursuant to any legal requirement. The fact that a person or entity has voluntarily submitted information pursuant to the CII Act of 2002 does not constitute compliance with any requirement to submit that information or any other such information to a Federal agency under any other provision of law. Moreover, when information is required to be submitted to a Federal agency to satisfy a provision of law, it is not to be marked by the submitter, by DHS, or by any other party, as submitted or protected under the CII Act of 2002 or to be otherwise afforded the protections of the CII Act of 2002.

(b) *Freedom of Information Act disclosure exemptions.* Information that is separately exempt from disclosure under the Freedom of Information Act or applicable State or local law does not lose its separate exemption protection due to the applicability of these procedures or any failure to follow them.

(c) *Restriction on use of protected CII by regulatory and other federal agencies.* No Federal agency shall request, obtain, maintain, or use information protected under the CII Act of 2002 as a substitute for the exercise of its own legal authority to compel access to or submission of such information. Federal agencies shall not utilize CII for regulatory purposes without the written consent of the submitter.

(d) *Independently obtained information.* These procedures shall not be construed to limit or in any way affect the ability of a Federal, State, or local Government entity, agency, or authority, or any third party, under applicable law, to obtain information by means of a different law, regulation, rule, or other authority.

(e) *No private rights or privileges.* Nothing contained in these procedures is intended to confer any substantive or procedural right or privilege on any person or entity. Nothing in these procedures shall be construed to create a private right of action for enforcement of any provision of these procedures or a defense to noncompliance with any independently applicable legal obligation.

§ 29.4 Critical Infrastructure Information Program administration.

(a) *IAIP Directorate Program Management.* The Secretary of the Department of Homeland Security shall designate the Under Secretary of the Information Analysis Infrastructure Protection (IAIP) Directorate as the senior DHS official responsible for the direction and administration of the Critical Infrastructure Information Program.

(b) *Appointment of CII Program Manager.* The Under Secretary of IAIP shall:

(1) Appoint a CII Program Manager within the IAIP Directorate to direct and administer the CII Program;

(2) Commit necessary resources to the effective implementation of the CII Program; and

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

(c) *Appointment of CII Officers.* The CII Program Manager shall establish procedures to ensure that any DHS component or other entity that works with Protected CII appoints one or more employees to serve as a CII Officer for the activity in order to provide proper management and oversight. Persons appointed to these positions shall be fully familiar with these procedures.

(d) *Responsibilities of a CII Officer.* The CII Officer shall:

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

(2) Establish and maintain an ongoing self-inspection program, to include periodic review and assessment of the entity's storage, handling, and use of Protected CII;

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

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

(e) *Critical Infrastructure Information Management System (CIIMS).* The CII Program Manager shall develop and use an electronic database, to be known as the “Critical Infrastructure Information Management System” (CIIMS), to record the receipt, acknowledgement, validation, storage, destruction, and disclosure of Protected CII. This compilation of CII shall be protected by the provisions of the CII Act of 2002.

§ 29.5 Authority to receive Critical Infrastructure Information.

(a) The Secretary of Homeland Security shall designate the DHS IAIP Directorate as the sole entity authorized to acknowledge and validate the receipt of Protected CII.

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

(1) Such information is voluntarily submitted either directly to the IAIP Directorate or indirectly to the DHS IAIP Directorate by submitting it to any Federal agency which then, pursuant to the submitter's express direction, forwards the information to the DHS IAIP Directorate;

(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, as evidenced below, and

(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 (15) calendar days of the