

be reproduced to the minimum extent necessary consistent with the need to carry out official duties, provided that the reproduced material is marked and protected in the same manner as the original material.

(d) *Disposal of information.* Material containing Protected CII shall be disposed of by any method that prevents unauthorized retrieval.

(e) *Transmission of information.* Protected CII shall be transmitted only by U.S. first class, express, certified, or registered mail, or through secure electronic means.

(f) Automated Information Systems that contain CII shall comply with the requirements of the Federal Information Security Management Act of 2002, 44 U.S.C. 3531–3538, implementing policy, and Office of Management and Budget Circular No. A–130, Appendix III.

#### § 29.8 Disclosure of information.

(a) *Authorization of access.* The Under Secretary of IAIP, or his or her designee, may choose to provide or authorize access to Protected CII when it is determined that this access supports a lawful and authorized Government purpose as enumerated in the CII Act of 2002, other law, regulation, or legal authority.

(b) *Federal, State and Local Government access.* The CII Program Manager may provide Protected CII to an employee of the Federal Government, or of a State or local government, provided that such information is shared for purposes of securing the critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or for another informational purpose relating to homeland security. Protected CII may be made available to a State or local government entity only pursuant to its express agreement with the Program Manager that acknowledges the understanding and responsibilities of the recipient.

(c) *Disclosure of information to Federal contractors.* Disclosure of Protected CII to Federal contractors may be made after a CII Officer certifies that the contractor is performing services in support of the purposes of DHS. The contractor shall safeguard Protected CII in accordance with these procedures. Contractors shall not further disclose Protected CII to any of their components, employees, or other contractors (including subcontractors) without the prior written approval of a CII Officer unless such disclosure is expressly authorized in writing by the submitter.

(d) *Further use or disclosure of information by State and Local governments.* (1) State and local governments receiving information marked “Protected Critical Infrastructure Information” shall not disclose that information to any other party, or remove any CII markings, without first obtaining authorization from the CII Program Manager, who shall be responsible for requesting and obtaining written consent for any such State or local government disclosure from the person or entity that submitted the information.

(2) The CII Program Manager may not authorize State and local governments to further disclose or distribute the information to another party unless the Program Manager first obtains the written consent of the person or entity submitting the information.

(3) State and local governments may use Protected CII only for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act.

(e) *Disclosure of information to appropriate entities and the general public.* The IAIP Directorate may provide advisories, alerts, and warnings to relevant companies, targeted sectors, other government entities, or the general public regarding potential threats to critical infrastructure as appropriate. In issuing a warning, the IAIP Directorate shall protect from disclosure the source of any voluntarily submitted CII that forms the basis for the warning; and any information that is proprietary, business-sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately in the public domain.

(f) *Access by Congress and whistleblower protection.* (1)(i) Pursuant to section 214(a)(1)(D) of the Homeland Security Act, Protected CII shall not, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or employee of the United States for purposes other than the purposes of the CII Act of 2002, except—

(A) In furtherance of an investigation or the prosecution of a criminal act; or

(B) When disclosure of the information is made—

(1) To either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee thereof or subcommittee of any such joint committee; or

(2) To the Comptroller General, or any authorized representative of the Comptroller General, in the course of

the performance of the duties of the General Accounting Office.

(ii) If any disclosure is made pursuant to these exceptions, prior written authorization must be obtained, in consultation with the DHS Office of the General Counsel, from the DHS Secretary, DHS Deputy Secretary, Under Secretary for IAIP, the DHS Inspector General, or the CII Program Manager.

(2) Consistent with the authority to disclose information for any purpose described in § 29.2(h), disclosure of Protected CII may be made, without the written consent of the person or entity submitting such information, to the DHS Inspector General, or to any other employee designated by the Secretary of Homeland Security. Disclosure may be made by any officer or employee of the United States who reasonably believes that such information:

(i) Evidences an employee's or agency's conduct in violation of criminal law, or any other law, rule, or regulation, affecting or relating to the protection of the critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, or reconstitution; or

(ii) Evidences mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety affecting or relating to the protection of the critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, or reconstitution.

(3) Disclosures of the above nature are authorized by law and therefore are not subject to penalty under section 214(f) of the Homeland Security Act of 2002.

(g) *Responding to requests made under the Freedom of Information Act or State/local information access laws.*

(1) Protected CII shall be treated as exempt from disclosure under the Freedom of Information Act and, if provided by the CII Program Manager, or the Program Manager's designee, to a State or local government agency, entity or authority, or an employee or contractor thereof, shall not be made available pursuant to any State or local law requiring disclosure of records or information. Any Federal, State, or local government agency with questions regarding the protection of Protected CII from public disclosure shall contact the CII Program Manager, who may in turn consult with the DHS Office of the General Counsel.

(2) These procedures do not limit or otherwise affect the ability of a State or local government entity, agency, or authority to obtain information directly from the same person or entity voluntarily submitting information to