

the manufacture, sale, use, or operation of anti-terrorism technology for which a Designation is issued (regardless of whether such contract is entered into before or after the issuance of such Designation), including, without limitation, an independent laboratory or other entity engaged in testing or verifying the safety, utility, performance, or effectiveness of such technology, or the conformity of such technology to the Seller's specifications.

Designation—The term “Designation” means a designation of a qualified anti-terrorism technology under the SAFETY Act issued by the Under Secretary under authority delegated by the Secretary of Homeland Security.

Loss—The term “loss” means death, bodily injury, or loss of or damage to property, including business interruption loss (which is a component of loss of or damage to property).

Noneconomic damages—The term “noneconomic damages” means damages for losses for physical and emotional pain, suffering, inconvenience, physical impairment, mental anguish, disfigurement, loss of enjoyment of life, loss of society and companionship, loss of consortium, hedonic damages, injury to reputation, and any other nonpecuniary losses.

Physical harm—The term “physical harm” as used in the Act shall mean a physical injury to the body that caused, either temporarily or permanently, partial or total physical disability, incapacity or disfigurement. In no event shall physical harm include mental pain, anguish, or suffering, or fear of injury.

Qualified Anti-Terrorism Technology (QATT)—The term “qualified anti-terrorism technology” means any product, equipment, service (including support services), device, or technology (including information technology) designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause, for which a Designation has been issued under this Part.

SAFETY Act or Act—The term “SAFETY Act” or “Act” means the Support Anti-terrorism by Fostering Effective Technologies Act of 2002, enacted

as Subtitle G of Title VIII of the Homeland Security Act of 2002, Public Law 107-296.

Seller—The term “Seller” means any person or entity to whom or to which (as appropriate) a Designation has been issued under this Part (unless the context requires otherwise).

Under Secretary—The term “Under Secretary” means the Under Secretary for Science and Technology of the Department of Homeland Security.

PART 29—PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

Sec.

- 29.1 Purpose and scope.
- 29.2 Definitions.
- 29.3 Effect of provisions.
- 29.4 Protected Critical Infrastructure Information Program administration.
- 29.5 Requirements for protection.
- 29.6 Acknowledgment of receipt, validation, and marking.
- 29.7 Safeguarding of Protected Critical Infrastructure Information.
- 29.8 Disclosure of Protected Critical Infrastructure Information.
- 29.9 Investigation and reporting of violation of Protected CII procedures.

AUTHORITY: Pub. L. 107-296, 116 Stat. 2135 (6 U.S.C. 1 *et seq.*); 5 U.S.C. 301.

SOURCE: 69 FR 8083, Feb. 20, 2004, unless otherwise noted.

§ 29.1 Purpose and scope.

(a) *Purpose of the rule.* This part implements section 214 of Title II, Subtitle B, of the Homeland Security Act of 2002 through the establishment of uniform procedures for the receipt, care, and storage of Critical Infrastructure Information (CII) voluntarily submitted to the Federal government through the Department of Homeland Security. Title II, Subtitle B, of the Homeland Security Act is referred to herein as the Critical Infrastructure Information Act of 2002 (CII Act of 2002). Consistent with the statutory mission of the Department of Homeland Security (DHS) to prevent terrorist attacks within the United States and reduce the vulnerability of the United States to terrorism, it is the policy of DHS to encourage the voluntary submission of CII by safeguarding and protecting that information from unauthorized disclosure and

by ensuring that such information is expeditiously and securely shared with appropriate authorities including Federal national security, homeland security, and law enforcement entities and, consistent with the CII Act of 2002, with State and local officials, where doing so may reasonably be expected to assist in preventing, preempting, and disrupting terrorist threats to our homeland. As required by the CII Act of 2002, the procedures established herein include mechanisms regarding:

(1) The acknowledgement of receipt by DHS of voluntarily submitted CII;

(2) The maintenance of the identification of CII voluntarily submitted to DHS for purposes of, and subject to the provisions of the CII Act of 2002;

(3) The receipt, handling, storage, and proper marking of information as Protected CII;

(4) The safeguarding and maintenance of the confidentiality of such information that permits the sharing of such information within the Federal government and with foreign, State, and local governments and government authorities, and the private sector or the general public, in the form of advisories or warnings; and

(5) The issuance of notices and warnings related to the protection of critical infrastructure and protected systems in such a manner as to protect from unauthorized disclosure the identity of the submitting person or entity as well as information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is not customarily available in the public domain.

(b) *Scope.* These procedures apply to all Federal agencies that handle, use, or store Protected CII pursuant to the CII Act of 2002. In addition, these procedures apply to United States Government contractors, to foreign, State, and local governments, and to government authorities, pursuant to any necessary express written agreements, treaties, bilateral agreements, or other statutory authority.

§ 29.2 Definitions.

For purposes of this part:

Critical Infrastructure has the definition referenced in section 2 of the Homeland Security Act of 2002 and

means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Critical Infrastructure Information, or CII means information not customarily in the public domain and related to the security of critical infrastructure or protected systems. CII consists of records and information concerning:

(1) Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms the interstate commerce of the United States, or threatens public health or safety;

(2) The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation, risk-management planning, or risk audit; or

(3) Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

Critical Infrastructure Information Program, or CII Program means the maintenance, management, and review of these procedures and of the information provided to DHS in furtherance of the protections provided by the CII Act of 2002.

Information Sharing and Analysis Organization, or ISAO means any formal or informal entity or collaboration created or employed by public or private sector organizations for purposes of:

(1) Gathering and analyzing CII in order to better understand security

problems and interdependencies related to critical infrastructure and protected systems in order to ensure the availability, integrity, and reliability thereof;

(2) Communicating or sharing CII to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or incapacitation problem related to critical infrastructure or protected systems; and

(3) Voluntarily disseminating CII to its members, Federal, State, and local governments, or to any other entities that may be of assistance in carrying out the purposes specified in this section.

Local Government has the same meaning as is established in section 2 of the Homeland Security Act of 2002 and means:

(1) A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a non-profit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government;

(2) An Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and

(3) A rural community, unincorporated town or village, or other public entity.

Protected Critical Infrastructure Information, or Protected CII means CII (including the identity of the submitting person or entity) that is voluntarily submitted to DHS for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement as described in § 29.5. This information maintains its protected status unless DHS's Protected CII Program Manager or the Protected CII Program Manager's designees render a final decision that the information is not Protected CII.

Protected System means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a fa-

cility of critical infrastructure and includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.

Purpose of CII has the meaning set forth in section 214(a)(1) of the CII Act of 2002 and includes the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose.

Submission to DHS as referenced in these procedures means any transmittal of CII to the DHS Protected CII Program Manager or the Protected CII Program Manager's designees, as set forth in § 29.5.

Voluntary or Voluntarily, when used in reference to any submission of 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 by an ISAO acting on behalf of its members. 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. 781(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 accompanies the solicitation of an offer or a sale of securities. The term also explicitly excludes information or statements submitted during a regulatory proceeding or relied upon as a basis for making licensing or permitting determinations.

§ 29.3 Effect of provisions.

(a) *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 DHS pursuant to a Federal legal requirement, nor do they pertain to any obligation of any Federal agency to disclose mandatorily submitted information (even where it is identical to information voluntarily submitted to DHS pursuant to the CII Act of 2002). 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 to a Federal agency under any other provision of law. Information submitted to any other Federal agency pursuant to a Federal legal requirement is not to be marked as submitted or protected under the CII Act of 2002 or otherwise afforded the protection of the CII Act of 2002, provided, however, that such information, if it is separately submitted to DHS pursuant to these procedures, may upon submission to DHS be marked as Protected CII or 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 that same information. Federal agencies shall not utilize Protected CII for regulatory purposes without the written consent of the submitter or another party on the submitter's behalf.

(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 otherwise obtain CII by means of a different law, regulation, rule, or other authority, including such information as is lawfully and custom-

arily disclosed to the public. Independently obtained information does not include any information derived directly or indirectly from Protected CII subsequent to its submission. Nothing in these procedures shall be construed to limit or in any way affect the ability of such entities, agencies, authorities, or third parties to use such information in any manner permitted by law.

(e) *No private right of action.* 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 Protected Critical Infrastructure Information Program administration.

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

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

(1) Appoint a Protected CII Program Manager within the IAIP Directorate who is responsible to the Under Secretary for the administration of the Protected CII Program;

(2) Commit resources necessary to the effective implementation of the Protected CII 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 Protected CII Program to facilitate the expeditious and secure sharing with appropriate authorities, including Federal national security, homeland security, and law enforcement entities and, consistent with the CII Act of 2002, with State and local officials, where doing so may reasonably be expected to

§ 29.5

6 CFR Ch. I (1–1–05 Edition)

assist in preventing, preempting, or disrupting terrorist threats to our homeland; and

(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

Protected CII Program Manager's designees shall be responsible for reviewing all submissions that request protection under the CII Act of 2002. The Protected CII Program Manager or the Protected CII Program Manager's designee shall review the submitted information as soon as practicable. If a determination is made that the submitted information meets the requirements for protection, the Protected CII Program Manager or the Protected CII Program Manager's designee shall mark the information as required in paragraph (c) of this section, and disclose it only pursuant to § 29.8.

(2) If the Protected CII Program Manager or the Protected CII Program Manager's designees make an initial determination that the information submitted does not meet the requirements for protection under the CII Act of 2002, the Protected CII Program Manager or the Protected CII Program Manager's designees 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 Protected CII Program Manager or the Protected CII Program Manager's designees will review any further information provided before rendering a final determination;

(C) Provide the submitter with an opportunity to withdraw the submission;

(D) Notify the submitter that any response to the notification must be received by the Protected CII Program Manager or the Protected CII Program Manager's designees no later than thirty calendar days after the date of the notification; and

(E) Request the submitter to state whether, in the event the Protected CII Program Manager or the Protected CII Program Manager's designees make 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 Protected CII Program Manager or the Protected CII Program Manager's designees, after following the procedures set forth in paragraph (e)(2)(i) of this section, make a final determination that the information is not Protected CII, the Protected CII Program Manager or the Protected CII Program Manager's designees, in accordance with the submitter's written preference, shall maintain the information without protection or following coordination, as appropriate, with other Federal national security, homeland security, or law enforcement authorities, destroy it in accordance with the Federal Records Act unless the Protected CII Program Manager or the Protected CII Program Manager's designees, consistent with the coordination required in this subpart, determine there is a need to retain it for law enforcement and/or national security reasons. The Protected CII Program Manager or the Protected CII Program Manager's designees shall destroy the information within thirty calendar days of making a final determination. If the submitter, however, cannot be notified or the submitter's response is not received within thirty calendar days after the submitter received the notification, as provided in paragraph (e)(2)(i) of this section, the Protected CII Program Manager or the Protected CII Program Manager's designee will destroy the information in accordance with the Federal Records Act, unless the Protected CII Program Manager or the Protected CII Program Manager's designee, after coordination with other Federal national security, homeland security, or law enforcement authorities, as appropriate, determines that there is a need to retain it for law enforcement and/or national security reasons.

(f) *Changing the status of Protected CII to non-Protected CII.* Once information is validated, only the Protected CII Program Manager or the Protected CII Program Manager's designees may change the status of Protected CII to that of non-Protected CII and remove its Protected CII markings. Status

changes may take place when the submitter requests in writing that the information no longer be protected under the CII Act of 2002 or when the Protected CII Program Manager or the Protected CII Program Manager's designee determines that the information was customarily in the public domain, is publicly available through legal means, or is required to be submitted to DHS by Federal law or regulation. The Protected CII Program Manager or the Protected CII Program Manager's designees shall inform the submitter when a change in status is made. Notice of the change in status of Protected CII shall be provided to all recipients of that Protected CII under § 29.8.

§ 29.7 Safeguarding of Protected Critical Infrastructure Information.

(a) *Safeguarding.* 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 by appropriate storage and handling. 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.* When Protected CII is in the physical possession of a person, reasonable steps shall be taken to minimize the risk of access to Protected CII by unauthorized persons. When Protected CII is not in the physical possession of a person, it shall be stored in a secure environment that affords it the necessary level of protection commensurate with its vulnerability and sensitivity.

(c) *Reproduction.* Pursuant to procedures prescribed by the Protected CII Program Manager, a document or other material containing PCII may be reproduced to the extent necessary consistent with the need to carry out official duties, provided that the reproduced documents or material are marked and protected in the same manner as the original documents or material.

(d) *Disposal of information.* Documents and material containing Protected CII may be disposed of by any method that prevents unauthorized retrieval.

(e) *Transmission of information.* Protected CII shall be transmitted only by secure means of delivery as determined by the Protected CII Program Manager or the Protected CII Program Manager's designees.

(f) *Automated Information Systems.* The Protected CII Program Manager or the Protected CII Program Manager's designees shall establish security requirements for Automated Information Systems that contain Protected CII.

§ 29.8 Disclosure of Protected Critical Infrastructure Information.

(a) *Authorization of access.* The Under Secretary for IAIP, or the Under Secretary's 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. Any disclosure or use of Protected CII within the Federal government is limited by the terms of the CII Act of 2002. Accordingly, any advisories, alerts, or warnings issued to the public pursuant to paragraph (e) of this section shall protect from disclosure:

(1) The source of any voluntarily submitted CII that forms the basis for the warning, and

(2) Any information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is not customarily in the public domain.

(b) *Federal, State, and local government sharing.* The Protected CII Program Manager or the Protected CII Program Manager's designees 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 including, without limitation, the identification, analysis, prevention, preemption, and/or disruption of terrorist threats to our homeland. Protected CII may be provided to a State or local government entity only pursuant to its express written

agreement with the Protected CII Program Manager to comply with the requirements of paragraph (d) of this section and 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 only after the Protected CII Program Manager or a Protected CII Officer certifies that the contractor is performing services in support of the purposes of DHS, the contractor has signed corporate or individual confidentiality agreements as appropriate, covering an identified category of contractor employees where appropriate, and has agreed by contract to comply with all the requirements of the Protected CII Program. The contractor shall safeguard Protected CII in accordance with these procedures and shall not remove any “Protected CII” markings. Contractors shall not further disclose Protected CII to any of their components, additional employees, or other contractors (including subcontractors) without the prior written approval of the Protected CII Program Manager or the Protected CII Program Manager’s designees, unless such disclosure is expressly authorized in writing by the submitter and is the subject of timely notification to the Protected CII Program Manager.

(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 share that information with any other party, or remove any Protected CII markings, without first obtaining authorization from the Protected CII Program Manager or the Protected CII Program Manager’s designees 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 or on whose behalf the information was submitted.

(2) The Protected CII Program Manager or a Protected CII Program Manager’s designee may not authorize State and local governments to further disclose the information to another party unless the Protected CII Pro-

gram Manager or a Protected CII Program Manager’s designee 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 or to the general public.* The IAIP Directorate may provide advisories, alerts, and warnings to relevant companies, targeted sectors, other governmental entities, ISAOs or the general public regarding potential threats and vulnerabilities to critical infrastructure as appropriate. In issuing a warning, the IAIP Directorate shall protect from disclosure the source of any Protected CII that forms the basis for the warning as well as any information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is not customarily in the public domain.

(f) *Access by Congress and whistleblower protection.* (1) Exceptions for disclosure.

(i) Pursuant to section 214(a)(1)(D) of the CII Act of 2002, 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 officer or employee of the United States makes any disclosure pursuant to these exceptions, contemporaneous written notification must be provided to the Department through the Protected CII Program Manager.

(2) Consistent with the authority to disclose information for any purpose described in § 29.2, 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.

(3) Subject to the limitations of title 5 U.S.C., section 1213 (the “Whistleblower Protection Act”), disclosure of Protected CII 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.

(4) Disclosures of all of the information cited in paragraphs (f)(1) through (3) of this section, including under paragraph (f)(1)(i)(A), 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 Protected CII Program Manager or the Protected CII Program Manager’s designees 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 Protected CII Program Manager, who shall in turn con-

sult 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 under applicable State or local law information directly from the same person or entity voluntarily submitting information to DHS. Information independently obtained by a State or local government entity, agency, or authority is not subject to the CII Act of 2002’s prohibition on making such information available pursuant to any State or local law requiring disclosure of records or information.

(h) *Ex parte communications with decisionmaking officials.* Pursuant to section 214(a)(1)(B) of the Homeland Security Act of 2002, Protected CII is not subject to any agency rules or judicial doctrine regarding ex parte communications with a decision making official.

(i) *Restriction on use of Protected CII in civil actions.* Pursuant to section 214(a)(1)(C) of the Homeland Security Act of 2002, Protected CII shall not, without the written consent of the person or entity submitting such information, be used directly by any Federal, State, or local authority, or by any third party, in any civil action arising under Federal or State law if such information is submitted in good faith under the CII Act of 2002.

(j) *Disclosure to foreign governments.* The Protected CII Program Manager or the Protected CII Program Manager’s designees may provide Protected CII to a foreign Government without the written consent of the person or entity submitting such information to the same extent, and under the same conditions, it may provide advisories, alerts, and warnings to other governmental entities as described in paragraph (e) of this section, or in furtherance of an investigation or the prosecution of a criminal act. Before disclosing Protected CII to a foreign government, the Protected CII Program Manager or the Protected CII Program Manager’s designees shall protect from disclosure the source of the Protected CII, any information that is proprietary or business sensitive, relates specifically to the

submitting person or entity, or is otherwise not appropriate for such disclosure.

(k) *Obtaining written consent for further disclosure from the person or entity submitting information.* (1) Authority to Seek and Obtain Submitter's Consent to Disclosure. The Protected CII Program Manager or any Protected CII Program Manager's designee may seek and obtain written consent from persons or entities submitting information when such consent is required under the CII Act of 2002 to permit disclosure. In exigent circumstances, and so long as contemporaneous notice is provided to the Protected CII Program Manager or the Protected CII Program Manager's designees, any Federal government employee may seek the consent of the submitting party to the disclosure of Protected CII where such consent is required under the CII Act of 2002.

(2) *Consequence of Consent.* Whether given in response to a request from the Protected CII Program Manager, the Protected CII Program Manager's designees, or another Federal government employee pursuant to paragraph (k)(1) of this section, a person's or entity's consent to additional disclosure, if conditioned on a limited release of Protected CII that is made for DHS's purposes and in a manner that offers reasonable protection against disclosure to the general public, shall not result in the information's loss of treatment as Protected CII.

§ 29.9 Investigation and reporting of violation of protected CII procedures.

(a) *Reporting of possible violations.* Persons authorized to have access to Protected CII shall report any possible violation of security procedures, the loss or misplacement of Protected CII, and any unauthorized disclosure of Protected CII immediately to the Protected CII Program Manager or the Protected CII Program Manager's designees who shall in turn report the incident to the IAIP Directorate Security Officer and to the DHS Inspector General.

(b) *Review and investigation of written report.* The Inspector General, Protected CII Program Manager, or IAIP Security Officer shall investigate the incident and, in consultation with the DHS Office of the General Counsel, determine whether a violation of procedures, loss of information, and/or unauthorized disclosure has occurred. If the investigation reveals any evidence of wrongdoing, DHS, through its Office of the General Counsel, shall immediately contact the Department of Justice's Criminal Division for consideration of prosecution under the criminal penalty provisions of section 214(f) of the CII Act of 2002.

(c) *Notification to originator of Protected CII.* If the Protected CII Program Manager or the IAIP Security Officer determines that a loss of information or an unauthorized disclosure has occurred, the Protected CII Program Manager or the Protected CII Program Manager's designees shall notify the submitter of the information in writing, unless providing such notification could reasonably be expected to harm the investigation of that loss or any other law enforcement, national security, or homeland security interest. The written notice shall contain a description of the incident and the date of disclosure, if known.

(d) *Criminal and administrative penalties.* As established in section 214(f) of the CII Act, whoever, being an officer or employee of the United States or of any department or agency thereof, knowingly publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information protected from disclosure by the CII Act of 2002 and coming to the officer or employee in the course of his or her employment or official duties or by reason of any examination or investigation made by, or return, report, or record made to or filed with, such department or agency or officer or employee thereof, shall be fined under title 18 of the United States Code, imprisoned not more than one year, or both, and shall be removed from office or employment.