DEPARTMENT OF HOMELAND SECURITY

6 CFR Part 29

RIN 1601–AA14

Procedures for Handling Critical Infrastructure Information

AGENCY: Office of the Secretary, Homeland Security.

ACTION: Notice of proposed rulemaking.

SUMMARY: This notice of proposed rulemaking establishes for Federal agencies the uniform procedures to implement Section 214 of the Homeland Security Act of 2002 regarding the receipt, care, and storage of Critical Infrastructure Information (CII) voluntarily submitted to the Federal Government. The protection of critical infrastructure reduces the vulnerability of the United States to acts of terrorism.

DATES: Written comments on this notice of proposed rulemaking may be submitted to the Department of Homeland Security on or before June 16, 2003.

ADDRESSES: Submit written comments (preferably an original and three copies) to Associate General Counsel (General Law), Department of Homeland Security, Washington, DC 20528. Electronic comments may be submitted to *cii.regcomments@DHS.gov.*

FOR FURTHER INFORMATION CONTACT: Frank Nolan, (202) 282–8495, not a toll free call.

SUPPLEMENTARY INFORMATION:

I. Background

On November 25, 2002, the President signed into law the Homeland Security Act (Pub. L. 107–296), which created the new Department of Homeland Security (DHS) and established its responsibilities. Pursuant to the provisions of the Act, the Department came into existence on January 24, 2003.

The responsibilities of the Department include the taking of action to prevent terrorist attacks within the United States and to reduce the vulnerability of the United States to acts of terrorism. The reduction of that vulnerability includes the protection of vital physical or computer-based systems and assets, collectively referred to as ''critical infrastructure,'' the incapacitation or destruction of which would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of these matters. The Department of Homeland Security recognizes the importance of receiving information from those with direct knowledge on the security of that critical infrastructure in order to reduce the vulnerability of this critical infrastructure to acts of terrorism.

The Department recognizes that its receipt of information pertaining to the security of critical infrastructure, much of which is not customarily within the public domain, is best encouraged through the assurance that such information will be utilized for securing the United States and will not be disseminated to the general public. Accordingly, section 214 of the Homeland Security Act, subtitle B of Title 2, which is referenced as the Critical Infrastructure Information Act of 2002 (''CII Act''), provides for the establishment of a critical infrastructure protection program that protects from disclosure to the general public any critical infrastructure information which the public may voluntarily provide to the Department.

Although the Homeland Security Act establishes a working definition of critical infrastructure information, the Department relies upon the discretion of the submitter as to whether the volunteered information meets the definition of critical infrastructure information. These procedures establish how critical infrastructure information volunteered by the public will be protected pursuant to section 214 of the Homeland Security Act.

II. Notice of Proposed Rulemaking

This notice of proposed rulemaking establishes the procedures for protecting critical infrastructure information which are referenced in section 214(e) of the CII Act of 2002.

This regulation establishes uniform procedures for the receipt, care, and storage of Critical Infrastructure Information (CII) voluntarily provided to the Federal Government by the public. These procedures apply to all Federal agencies that receive, care for, or store CII that is voluntarily submitted to the Federal Government pursuant to the CII Act of 2002. 6 U.S.C. 130, *et seq.* In addition, these procedures apply to United States Government contractors, to Foreign, State, and local governments, and to government authorities, pursuant to their express agreements.

III. Procedural Requirements

In recognition of the importance of these procedures, the Department is providing this notice of proposed rulemaking of uniform procedures for the receipt, care, and storage of voluntarily submitted CII. As these procedures will affect Federal, State, and local governments and entities, the Department recognizes the importance of providing the opportunity for comment upon these procedures by both the government and private sector.

Executive Order 12866

It has been determined that this rulemaking is a significant regulatory action for purposes of section 3(f)(4) of Executive Order 12866. This rulemaking is, however, not considered an economically significant regulatory action for the purposes of Executive Order 12866. This rulemaking has been reviewed and approved by the Office of Management and Budget.

Regulatory Flexibility Act Certification

Because no notice of proposed rulemaking is required, the provisions of the Regulatory Flexibility Act (5 U.S.C. chapter 6) do not apply.

Paperwork Reduction Act of 1995

OMB does not consider nonspecific or nondirective reporting—such as the information requested in the rule—that the respondent wishes to provide on a specific topic without further specification being sought to be subject to the Paperwork Reduction Act.

List of Subjects in 6 CFR Part 29

Classified information, Confidential business information, Reporting and recordkeeping requirements.

Authority and Issuance

For the reasons set forth above, 6 CFR is proposed to be amended by adding part 29 to read as follows:

PART 29—CRITICAL INFRASTRUCTURE INFORMATION

Sec.

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

§ 29.1 Purpose and Scope.

(a) *Purpose.* 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. Title II, Subtitle B, of the Homeland Security Act is referred to herein as the CII Act of 2002. It is Department of Homeland Security (DHS) policy to encourage the voluntary submission of CII by protecting that information from unauthorized disclosure to the fullest extent permitted by law. As required by the CII Act of 2002, the procedures established herein include mechanisms regarding:

(1) The acknowledgement of receipt by a Federal agency of critical infrastructure information voluntarily submitted to the Federal Government;

(2) The maintenance of the identification of critical infrastructure information voluntarily submitted to the Federal Government for purposes of and subject to the provisions of the CII Act of 2002;

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

(4) The protection 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

(5) The issuance of notices and warnings related to the protection of critical infrastructure and protected systems in such a manner to protect from public 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/or is not appropriately in the public domain.

(b) *Scope.* These procedures apply to all Federal agencies that receive, care for, or store CII voluntarily submitted to the Federal Government pursuant to the CII Act of 2002. In addition, these procedures apply to United States Government contractors, to Foreign, State, and local governments, and government authorities, pursuant to their express agreements.

§ 29.2 Definitions.

For purposes of this part:

(a) *Critical Infrastructure* has the same definition as described 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 thereof.

(b) *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 or information concerning:

(1) Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by 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 thereto, 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.

(c) *Critical Infrastructure Information Program or ''CII Program''* means the maintenance, management, and review of these procedures and of the information provided to DHS in expectation of the protections provided by the CII Act of 2002.

(d) *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 critical infrastructure information in order to better understand security problems and interdependencies related to critical infrastructure and protected systems to ensure the availability, integrity, and reliability thereof;

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

(3) Voluntarily disseminating critical infrastructure information to its members, Federal, State, and local governments, or any other entities that may be of assistance in carrying out the purposes specified in paragraphs (d)(1) and (d)(2) of this section.

(e) *Local Government* has the same meaning as 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 nonprofit 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.

(f) *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 of this chapter. This information maintains its protected status unless the CII Program Manager renders a final decision that the information is not Protected CII.

(g) *Protected System* means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility 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.

(h) *Purpose* has the meaning as described 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.

(i) *Submission to DHS* as referenced in these procedures means any transmittal of CII from any entity to DHS. The CII may be provided to DHS either directly or indirectly via another Federal agency, which, upon receipt of the CII, will forward it to DHS.

(j) *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 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

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

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

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 decision-making 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 Critical Infrastructure Information in civil actions.* Protected CII shall not, without the written consent of the person or entity submitting such information, be used 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 for homeland security purposes.

(j) *Disclosure to foreign governments.* The CII Program Manager, or the Program Manager's designee, may provide Protected CII to a Foreign Government without the written consent of the person or entity submitting such information to the same extent it may provide advisories, alerts, and warnings to other governmental entities as described in § 29.8(e) of this chapter, or in furtherance of an investigation or the prosecution of a criminal act.

(k) *Obtaining written consent for further disclosure from the person or entity submitting information.* Only the CII Program Manager, or the 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. A person or entity's consent to additional disclosure, if conditioned both on a limited release of Protected CII 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 CII procedures.

(a) All persons authorized to have access to Protected CII shall report any possible violations of security procedures, the loss or misplacement of Protected CII, and any unauthorized disclosure of Protected CII immediately to the CII Program Manager, 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, CII Program Manager, or IAIP Security Officer, shall investigate the incident and, in consultation with the 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 the Office of the General Counsel, shall immediately contact the Department of Justice, 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 CII Program Manager or the IAIP Security Officer determines that an unauthorized disclosure occurred, or that Protected CII is missing, the CII Program Manager shall notify the submitter of the information in writing. The written notice shall contain a description of the incident and the date of disclosure, if known.

(d) *Criminal and administrative penalties:* Pursuant to section 214(f) of the Homeland Security Act of 2002, 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 CII protected from disclosure by the Homeland Security Act 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 (1) year, or both, and shall be removed from office or employment.

Dated: April 9, 2003.

Tom Ridge,

Secretary of Homeland Security.

[FR Doc. 03–9126 Filed 4–14–03; 8:45 am]

BILLING CODE 4410–10–P