DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 29

RIN 1601–AA14

Procedures for Handling Critical Infrastructure Information

AGENCY: Office of the Secretary, DHS.

ACTION: Final rule.

SUMMARY: This final rule amends the February 2004 Interim Rule establishing uniform procedures to implement the Critical Infrastructure Information Act of 2002. These procedures govern the receipt, validation, handling, storage, marking, and use of critical infrastructure information voluntarily submitted to the Department of Homeland Security. The procedures are applicable to all Federal, State, local, and tribal government agencies and contractors that have access to, handle, use, or store critical infrastructure information that enjoys protection under the Critical Infrastructure Information Act of 2002.

DATES: *Effective Date:* This final rule is effective September 1, 2006.

FOR FURTHER INFORMATION CONTACT: Laura Kimberly, Directorate for Preparedness (202) 360–3023, not a toll-free call.

SUPPLEMENTARY INFORMATION:

Table of Contents

PART 29—PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

Table of Abbreviations

In this document, the following abbreviations are commonly used:

APA—Administrative Procedure Act
CII—Critical Infrastructure Information
CII Act—Critical Infrastructure Information Act of 2002
DHS—Department of Homeland Security
FOIA—Freedom of Information Act
HSA—Homeland Security Act of 2002
ISAO—Information Sharing and Analysis Organization
NPRM—Notice of Proposed Rulemaking
PCII—Protected Critical Infrastructure Information
PCIIMS—Protected Critical Infrastructure Information Management System

I. Introduction

The Critical Infrastructure Information Act of 2002 (CII Act) [1] is a crucial tool in facilitating the Department of Homeland Security's (DHS) analysis of infrastructure vulnerability and related information for planning, preparedness, warnings and other purposes. The CII Act enables DHS to collaborate effectively to protect America's critical infrastructure, eighty-five percent of which is in the private sector's hands. The CII Act authorized DHS to accept information relating to critical infrastructure from the public, owners and operators of critical infrastructure, and State, local, and tribal governmental entities, while limiting public disclosure of that sensitive information under the Freedom of Information Act, 5 U.S.C. 552 (FOIA), and other laws, rules, and processes.

In responding to comments and drafting this final rule, DHS has been careful to further the purposes of the Protected Critical Infrastructure Information (PCII) Program as an effective anti-terrorism tool while also carefully observing its limitations. For the PCII Program to be successful, DHS believes that the rule must be as clear and certain as possible, yet flexible to respond to changing conditions. Among other measures, this final rule:

- Clarifies that a submittal validated as PCII will not thereafter lose its protected status except under a very narrow set of circumstances (section 29.6(g));
- Requires that PCII will be shared only for the Homeland Security purposes specified in the statute and in no event for other collateral regulatory purposes (section 29.3(b));
- Provides the PCII Program Manager with the flexibility to designate certain types of infrastructure information as presumptively valid PCII in order to accelerate the validation process and provide greater certainty to potential submitters (section 29.6(f));
- Provides that submissions not validated as PCII be returned to the submitter or destroyed (section 29.6(e)(2)(ii));
- Provides for submission of CII for protection through DHS field representatives (section 29.5(a)(1));
- Identifies procedures for indirect submissions to DHS through other Federal agencies (sections 29.1(f), 29.5(a)(1), 29.6(b), (d)); and
- Simplifies the information submission process (section 29.6).

On April 15, 2003, DHS published a notice of proposed rulemaking (NPRM) regarding the establishment of the PCII Program. 68 FR 18523 (Apr. 15, 2003). Written comments were accepted through June 16, 2003. DHS received 117 sets of comments.

DHS subsequently published an interim rule on February 20, 2004 at 69 FR 8074. In the February 2004 Interim Rule, DHS responded to the public comments received in response to the initial NPRM and invited additional public comments. DHS received 32 sets of responsive comments from various entities, including trade organizations writing on behalf of their membership, private sector and public interest entities, one State government agency, and individual commenters. The comments may be reviewed at *http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0438.xml.*

[1] Homeland Security Act of 2002 (HSA) Pub. L. 108–275, tit. II, subtit. B, sec. 211, 116 Stat. 2135, 2150 (Nov. 25, 2002) (6 U.S.C. 131–134).

II. Major Issues in the February 2004 Interim Rule

DHS has resolved several major issues raised in public comments on the February 2004 Interim Rule. The following sections identify specific issues raised by commenters and describe how these issues have been resolved.

A. Indirect Submissions of PCII

The preamble to the February 2004 Interim Rule discussed ''indirect submission'' of CII. Section 29.2 of the NPRM [2] defined ''submission of CII to DHS,'' to include ''either directly or indirectly via another Federal agency, which, upon receipt of the CII will forward it to DHS.'' In section 29.5(b)(1), the proposed rule provided that CII would receive the protections of the CII Act only when the information was submitted either ''directly to the IAIP [Preparedness] Directorate or indirectly to the DHS IAIP Directorate by submitting it to any Federal agency which then * * * forwards the information to the DHS IAIP Directorate.'' Other provisions of the proposed rule specifically required submittals to be made to the PCII Program Manager, either directly or indirectly.

DHS responded to the public comments on indirect submission received in the February 2004 Interim Final Rule. The preamble stated that, in light of substantial concern about allowing indirect submissions, DHS had removed references to indirect submissions from the rule and made clear that submissions must be made to the PCII Program Manager or the PCII Program Manager's designees. At the same time, DHS noted that it had received comments voicing support for indirect submissions. These comments favored the NPRM original intent, which was to facilitate information sharing with the Federal government through established relationships between owners of the nation's critical infrastructure and those Federal agencies that are sector leaders for particular infrastructure. Accordingly, after the PCII Program had become operational, and pending further analysis, the final rule might allow for indirect submissions. The February 2004 Interim Rule invited additional public comment.

Twenty additional sets of comments on this subject were received. Nine commenters opposed allowing indirect submissions, citing such considerations as the restrictions imposed on the use of PCII, concerns about the protection of submitted CII within agencies other than DHS, the potential for confusion as to what other agencies may do with information in their possession, and the risk of an appearance that PCII had been misused. Six other commenters considered indirect submissions problematic and believed that permitting such submissions would require additional clarification or a system of checks and balances. On the other hand, five organizations warned that not allowing indirect submissions would run contrary to their normal information flow with Federal agencies other than DHS.

Upon considering these comments, DHS has concluded that certain Federal personnel outside the Program Manager's Office at DHS (''Program Office''), including certain DHS field representatives and certain personnel in other federal agencies, should be permitted to receive and forward CII to the Program Manager, but that (absent a categorical inclusion, discussed below at section III.F.) only the PCII Program Office within DHS will be authorized to make the decision as to whether to validate a submission as PCII. The PCII Program Manager will authorize personnel in Federal governmental entities other than the PCII Program Office to accept a submission on behalf of the Program Office, but only when such personnel are trained to ensure compliance with the requirements of this final rule. The PCII Program Manager will normally take this step only when the particular governmental entity: (1) Has appointed a PCII Officer; (2) has the necessary staff, who are trained in PCII procedures; (3) has implemented measures to comply with this final rule; and (4) has agreed that the PCII Program Office may at any time verify that agency's compliance with the Final Rule and other program requirements. *See* section 29.5. Note that this final rule does not restrict the authority of the Secretary or the PCII Program Manager to designate officials to receive CII or take other actions in exigent circumstances.

B. Definitional Issues Affecting Qualifying Information

According to section 214(a)(1) of the CII Act (6 U.S.C. 133(a)(1)), ''critical infrastructure information'' that is ''voluntarily submitted'' to a ''covered Federal agency'' (*i.e.*, DHS) for its use for the specified purposes, when accompanied by an ''express statement,'' qualifies for CII Act protections. Section 212(3) of the CII Act (6 U.S.C. 131(3)) defines ''critical infrastructure information'' to mean, in pertinent part, ''information not customarily in the public domain,'' and section 212(7) of the CII Act (6 U.S.C. 131(7)) defines ''voluntary.'' In the final rule, changes have been made to two definitions that are relevant to these statutory provisions, and corollary definitions have been added.

(1) In the Public Domain

In the preamble to the February 2004 Interim Rule, DHS declined to interpret further the meaning of ''information not customarily in the public domain.'' Three commenters on the February 2004 Interim Rule urged that this phrase be defined. In response, in section 29.2(d), DHS has defined ''in the public domain'' in part as ''information lawfully, properly and regularly disclosed generally or broadly to the public.'' This definition draws in part on section 214(c) of the CII Act (6 U.S.C. 133(c)), which stipulates that nothing in section 214 constrains the collection of critical infrastructure information ''including any information lawfully and properly disclosed generally or broadly to the public * * *.'' The new definition further identifies certain types of information that are considered not to be in the public domain—specifically, ''information regarding systems, facilities, or operational security, or that is proprietary, business sensitive, or which might be used to identify a submitting person or entity.''

(2) Voluntary or Voluntarily

The definition of ''voluntary'' in section 29.2 of this rule implements section 212(7)(A) of the CII Act (6 U.S.C. 131(7)(A)), which provides that a submittal of CII is not ''voluntary'' if such information is provided pursuant to the exercise of legal authority by DHS (the ''covered agency'') to compel access to or submission of the information. Four commenters argued for a broader disqualification of information submitted to other Federal agencies pursuant to such agencies' exercise of their legal authority. The language of sections 212(2) and 212(7)(A) of the CII Act (6 U.S.C. 131(2) and 131(7)(A)) do not support such a reading and DHS has not adopted it.

Whether information provided to the PCII Program manager is ''voluntarily submitted'' is to be determined at the time CII is submitted. The terms ''submitted'' and ''relied upon'' in section 212(7)(B)(ii) (6 U.S.C. 131(7)(B)(ii)) are both retrospective in nature. Both employ the past tense and both apply to actions before the date that information is submitted to the PCII

[2] For ease of reference, all references in this final rule to sections or paragraphs without full citation refer to sections and paragraphs of promulgated 6 CFR part 29.

Program Manager. As discussed below in section III, the provision in section 29.6(f) of the February 2004 Interim Rule allowing a change of status from ''Protected'' to ''non-Protected'' based on a subsequent requirement that the information be submitted to DHS has been eliminated. This does not mean that DHS could not obtain related CII available under other DHS legal authority later in time. It does mean, however, that the specific documents voluntarily submitted as PCII will not be publicly released. *See* section 214(c) of the CII Act (6 U.S.C. 133(c)).

Section 212(7)(B)(ii) of the CII Act (6 U.S.C. 131(7)(B)(ii)), excludes from the definition of ''voluntary,'' information or statements ''submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings.'' Neither the term ''licensing or permitting determinations'' nor ''regulatory proceedings'' is defined in the CII Act, and the CII Act does not state explicitly to whom the information or statements must have been submitted or which agency relied upon them. One commenter urged greater precision in the definition of ''voluntary,'' and many commenters expressed concern over the potential impact of the PCII Program in a ''regulatory'' context.

DHS agrees that the terms should be defined with greater precision. It is clear throughout the statute that the terms ''voluntary'' and ''voluntarily'' refer only to submissions intended to reach DHS. *See* section 212(2) of the CII Act (6 U.S.C. 131(2)) (''covered Federal Agency'' means the Department of Homeland Security); sections 212(7)(A), and 214(a)(1) of the CII Act (6 U.S.C. 131(7)(A), 133(a)(1)). Section 212(7)(B)(ii) of the CII Act (6 U.S.C. 131(7)(B)(ii)), incorporates the concept of ''voluntary submissions,'' which, by its definition, involves only submission to DHS. Subsection 212(7)(b)(ii) limits only the scope of a voluntary submission to DHS. Thus, it is reasonable and appropriate to interpret the terms ''licensing or permitting determinations'' and ''regulatory proceedings'' in section 212(7)(B)(ii) as referring to such activities within DHS and DHS has done so. This is fully consistent with other provisions of the CII Act (sections 212(c) and 212(d)). Any broader interpretation would be inconsistent with Congress' purpose in creating the Act and impossible to administer effectively. Indeed, it is difficult to imagine how DHS could feasibly determine if and when any ''information or statements'' in CII had been previously submitted to or relied upon by any Federal agency other than DHS or any State, local or tribal entity in any public or private proceeding throughout time.

Further, the definition has been altered to reflect that submissions may be accepted from a ''single state or local governmental entity; or a private entity or person; or by an ISAO acting on behalf of its members or otherwise'' to address confusion expressed by potential submitters based on unnecessarily narrow constructions of the definition of a submitter.

C. Protected and Non-Protected Information

Several issues have arisen as to what portions or aspects of submitted information should enjoy the protections of the CII Act, and under which circumstances information should enjoy protection.

(1) Portion Marking

The preamble to the February 2004 Interim Rule reported that although six public comments advocated a requirement for marking those portions of submitted information that are entitled to protection under the CII Act, DHS had concluded that ''portion marking'' should not be required. One commenter on the February 2004 Interim Rule contested this position. DHS has considered these comments but has not altered its conclusion. Accordingly, no portion marking will be required.

(2) Definition of PCII

The CII Act defines CII in section 212(3) (6 U.S.C. 131(3)). DHS believes that any information, statements or other material reasonably necessary to explain the CII, put the CII in context, or describe the importance or use of the CII are appropriately within the scope of the protections intended by the CII Act. Accordingly, the definition of ''Protected Critical Infrastructure Information,'' or ''PCII,'' in section 29.2(g) has been modified to reflect this clarification.

(3) Source of the Information

The definition of ''Protected Critical Infrastructure Information,'' or ''PCII'' in section 29.2 of the February 2004 Interim Rule provides that the ''identity of the submitting person or entity'' enjoys the protections of the CII Act in parity with the information submitted. Two comments expressed concern about the ''anonymity'' of those on whose behalf an Information Sharing and Analysis Organization (ISAO) might submit CII. DHS recognizes that information may be submitted on behalf of others by an ISAO or trade association. DHS agrees and section 29.2 has been amended to clarify that the Act's protections extend to the identities of those persons or entities on whose behalf the information was submitted and to any other information that could be used to discover such identities. Section 29.8(e), relating to disclosure of information to appropriate entities or to the general public, has been conformed.

(4) Interplay of Sections 214(a)(1)(C) and 214(c) of the CII Act

Questions have also arisen regarding the meaning of section 214(a)(1)(C) of the CII Act (6 U.S.C. 133(a)(1)(C)): PCII ''shall not, without written consent of the person or entity submitting such information, be used directly * * * in any civil litigation * * * if such information is submitted [to DHS] in good faith.'' The issue is whether information in the hands of submitters will, by virtue of voluntary submission to DHS under this provision, be unavailable for use in civil litigation. When CII is submitted and validated for protection under the Act, the information and documents provided, and drafts and copies thereof retained by the submitter(s) or person working with the submitter(s), as well as any discussions with DHS regarding the CII, shall be considered PCII and cannot be the subject of civil discovery or other direct use in any civil litigation without the submitter's consent. DHS interprets the statutory phrase ''any civil action'' in section 214(a)(1)(C) of the CII Act to include civil litigation in any form or forum whether the United States is or is not a party. DHS disagrees with the notion, suggested by some, that the statutory language would permit civil discovery of such information while prohibiting its use as evidence at trial. This dichotomy makes little sense. ''Discovery'' of the information in a civil action, with all it entails, is in fact ''direct'' use of the information. The Act is structured to spur owners of CII and others to evaluate and share CII vulnerabilities and other sensitive information with the Department. Creating a civil discovery loophole to the protections of the Act would impede such cooperation and be fundamentally inconsistent with the language and purposes of the Act.

It is also important to focus on section 214(c) of the CII Act (6 U.S.C. 133(c)). That provision indicates that the Act shall not ''be construed to limit or otherwise affect the ability of a State, local, or Federal government entity [or private litigant] * * * to obtain critical infrastructure information in a manner not covered by'' section 214(a) (6 U.S.C. 133(a)). While PCII, including the

opinions, evaluations, conclusions or analyses that were submitted, may not be used directly in civil litigation, independently existing factual information obtained independently by a civil litigant from sources other than the PCII can present a different question under section 214(c).

(5) Good Faith Submission of CII

Section 29.2(n) was inserted in response to a commenter's request for a definition of ''good faith.'' This new section provides that any information that could be reasonably considered CII information, as defined in the regulations, is submitted in good faith. The subsequent validation of such information as PCII by the PCII Program Office, or the inclusion of such information in a category of pre-validated information, definitively establishes the submission as having been made in good faith.

(6) Communications With the Submitting Person or Entity

Another matter that the February 2004 Interim Rule did not address is communications of the PCII Program Office, or of other authorized recipients of PCII, with the submitting person or entity about the submittal or the submitted information. Part of the purpose of the CII Act is to encourage frank and open discussion with DHS regarding CII. It would defeat the purpose of the Act to declare such exchanges as outside the context of PCII. Certain communications are specifically intended to perform the functions enumerated in sections 29.6(d), (e)(2) and (f), 29.8(e), and 29.9(c), or to inquire whether the submitting person or entity consents to disclosures of the submitted information. Changes to sections 29.8(c) and 29.8(d)(2), and new section 29.8(f)(1)(i)(B) fill the void by authorizing the disclosure of PCII by Federal government officers, employees, and contractors, as well as State, local, and tribal governmental entities in order to facilitate communications with a submitting person or an authorized person on behalf of a submitting entity, about a CII submission by that person or entity.

D. Loss of Protected Status

Section 29.6(f) of the February 2004 Interim Rule responded to comments by providing for changes from ''Protected'' to ''non-Protected'' status when the submitting person or entity requested the change in writing, or when the PCII Program Manager or his or her designee determined 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.'' Two commenters sought clarification of or a change to this section.

Two of these criteria allowing a loss of protected status have been removed by this final rule. First, the test that would allow a loss of protected status because the submitted information ''is publicly available through legal means'' has been deleted because the CII Act does not provide for a change in status on this ground. Second, as noted above in the discussion of the definition of ''voluntary or voluntarily,'' the test that would allow a loss of protected status because the submitted information ''is required to be submitted to DHS by Federal law or regulation'' has been eliminated. This change has been made because the definitional exclusion in section 212(7)(A) of the CII Act (6 U.S.C. 131(7)(A)), and the section 29.2 definition of ''voluntary or voluntarily'' refers expressly to the time of submittal and is thus retrospective only. This does not, of course, prevent DHS from using current or future authority to mandate submission of any information. However, prior voluntary submissions under the CII Act may only be utilized in accordance with the Act's provisions.

E. Sharing of PCII With Foreign Governments

Ten commenters expressed concerns about the February 2004 Interim Rule's provision on ''Disclosure to foreign governments'' in section 29.8(j). Some pointed to an ambiguity as to whether this subsection was intended to allow the sharing of PCII with foreign governments, without the consent of the submitting person or entity, to an extent greater than would result from the issuance of advisories, alerts and warnings under section 214(g) of the CII Act. Commenters argued that if that was the intent, it was unauthorized by the CII Act.

DHS envisions situations in which international cooperation is required to combat terrorism, and PCII may form part of a warning to a foreign governmental entity. In these cases, appropriate cooperation may be accomplished as a warning under section 214(g) of the CII Act. Accordingly, former section 29.8(j) is unnecessary and has been omitted.

F. Emergency Disclosure of PCII

One commenter noted that exceptions should be drafted into the final rule that allow for the disclosure of specific information when there is an emergency that threatens widespread injury or loss of life, and that such disclosure must not be contingent on the prior written consent of the submitter. In response to this comment, DHS has modified section 29.8(e) to permit the use of PCII in advisories, alerts, and warnings without the consent of the submitting person or entity, but prior to doing so, DHS must ''take appropriate actions to protect * * * information that is proprietary, business sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately in the public domain'' (section 214(g) of the CII Act (6 U.S.C. 133(g))).

III. Other Changes to the Rule by Section

A. Purpose and Scope: Section 29.1

The February 2004 Interim Rule provided that warnings could be issued by DHS that were predicated upon CII submissions provided that the ''identity'' of the submitter was protected and the disclosure did not result in the public dissemination of the submitter's business proprietary/sensitive information (*i.e.*, information that is not ''customarily available'' in the public domain). The requirement to protect the ''identity'' of the disclosure has been broadened to protect the ''source'' of information, as well as information that might be used to identify the submitting person or entity. This broader formulation tracks the language in section 214(g)(1) of the CII Act (6 U.S.C. 133(g)(1)). It also recognizes that there may be instances in which PCII is provided to DHS by an ISAO or trade association. In such a case, confidentiality should extend to both the submitter of the information (the ISAO or trade association) and to the individual that provided the CII to the ISAO for submission. This has become particularly important with the development of collaboration with industry-wide working groups and ISAOs. The phrase ''otherwise not appropriately in the public domain'' was drawn from section 214(g)(2) of the CII Act (6 U.S.C. 133(g)(2)), and replaces ''customarily available.'' This change is intended to conform the language in this final rule to the statute and to be more protective of an owner or operator's proprietary or business confidential information. Then relevant portions of the revised definition of ''in the public domain'' in section 29.2, discussed in detail in section II above, has been added to this section.

With respect to the ''Scope'' of the PCII rule set forth in section 29.1(b), five commenters asked for clarification of the interrelationship between the procedures established by this rule and the requirements for the handling of other types of homeland security

information, such as Sensitive Security Information (SSI). This rule covers CII voluntarily submitted to DHS when accompanied by the statutory express statement. While other Federal agencies are not required to participate in the PCII Program, those that do desire to participate must first undergo appropriate training programs and take necessary steps to adhere to the statute and these regulations to enable the owners of the information to receive the full protections for their CII provided for in the CII Act. When information that is voluntarily submitted to the Federal government meets the definition of SSI in 49 CFR part 1520 and is also designated as CII by the PCII Program Office, it will be marked and protected in accordance with these procedures as PCII, but can also enjoy SSI protection. To provide greater clarity, however, section 29.1(b) has been revised and simplified to reflect that these rules apply to anyone authorized to handle, use, or store PCII or that otherwise receives PCII.

B. Definitions: Section 29.2

Five commenters addressed one or more definitional questions. The comments suggested changes to defined terms and also noted that some important terms were not defined at all.

Critical Infrastructure and *Critical Infrastructure Information.* Several comments asked for a more explicit definition of these terms. The terms are defined in statutory language and no changes were made. For clarity, the statutory references on which section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101), was based have been included.

Protected Critical Infrastructure Information Program, or *PCII Program*. The previously defined term ''Critical Infrastructure Information Program'' has been replaced with the more descriptive term ''Protected Critical Infrastructure Information Program,'' or ''PCII Program.''

Information Sharing and Analysis Organization, or *ISAO*. Two comments concerning the anonymity of those on whose behalf an ISAO might submit are discussed in section II.C.(2) above. An additional comment specifically asked for clarification that ISAOs have the capability to make CII submissions on behalf of their sector participants. That comment does not require a change in the definition. The definition of the terms ''voluntary or voluntarily'' and ''Protected Critical Infrastructure Information,'' discussed below, make clear that ISAOs may submit CII on behalf of members.

Protected Critical Infrastructure Information, or *PCII*. This definition has been changed to make clear that the identities of both the original providers and subsequent submitters of information are included within PCII when an ISAO or trade association has submitted the CII for validation as PCII. The definition was also expanded to include any information that is necessary to explain or provide context for the PCII. In response to a comment, the last sentence of the definition in the February 2004 Interim Rule has been moved to section 29.6(b) because it contained a policy statement rather than an element of a definition.

Purposes of the CII Act. This term, which conforms with the usage at 6 CFR 29.5(a), is more apt than the previously defined ''purpose of CII.''

The terms ''*In the public domain*,'' ''*Regulatory proceeding*,'' ''*State*,'' ''*Submitted in good faith*'' and ''*Voluntary or voluntarily*'' are discussed in detail in Section II.

C. Effect of the Provisions: Section 29.3

Several commenters expressed concern that PCII could be used for purposes other than securing critical infrastructure, such as regulating workplace safety or monitoring compliance with environmental laws. Congress was very clear on this point in the CII Act, specifying a very narrow range of appropriate uses for PCII. Information in the PCII submission may be employed * * * regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery or reconstitution or other information purpose * * * Section 214(a)(1) of the CII Act (6 U.S.C. 133(a)(1)). Indeed, the statute expressly forbids use of PCII, and sets forth a criminal sanction, for purposes other than those specified in the Act. *See* section 241(a)(1)(D) of the CII Act (6 U.S.C. 133(a)(1)(D)) (noting also appropriate use ''in furtherance of a criminal investigation or in the prosecution of a criminal act,'' or when shared subject to these requirements with specified persons in the legislative branch); section 214(f) (6 U.S.C. 133(f)) (penalties). Section 213(a)(1)(E) expressly forbids state and local governments from disclosing or using PCII material ''other than for the purposes of protecting critical infrastructure or protected systems * * *''). *Id.*

These and other provisions of the CII Act are unambiguous; PCII may not be disseminated to other federal, state or local agencies for other regulatory purposes. Nor may any recipient of PCII utilize any information in the PCII for other regulatory purposes. The PCII Program Office will impose appropriate restrictions on all recipients of PCII, and will require appropriate training and oversight to ensure compliance with these legislative mandates.

Certain commenters have also suggested that an individual with collateral regulatory responsibility (*e.g.* worker health and safety) would not be able to segregate knowledge gained from PCII information (once learned) from his day-to-day duties on non-security issues, and thus would ''inevitably'' use such PCII information for non-security purposes. The PCII Program Office is aware of this concern and will take it into account when determining the appropriate persons with whom to share particular PCII. A person proposing to submit CII may consult with the PCII Program Office regarding appropriate restrictions applicable to use of the particular potential submission prior to making that submission.

D. PCII Program Administration: Section 29.4

Three commenters addressed the provisions of this section. Only one paragraph was changed. Paragraph (e) was modified from the February 2004 Interim Rule to make clear that the ''development'' of the Protected Critical Infrastructure Information Management System (PCIIMS) is the responsibility of the PCII Program Manager.

Three commenters suggested that the PCIIMS contain only what could be called the tracking data and that the actual PCII should be kept elsewhere. The suggestions will not be adopted. The tracking data may include information that identifies the submitter, and to the extent that it does, it is included in the revised definition of PCII (section 29.2) under the CII Act. DHS has an obligation to safeguard all PCII. Accordingly, DHS will maintain PCII according to a distributed model with information stored in a number of databases including the PCIIMS.

E. Requirements for Protection: Section 29.5

Eleven commenters addressed various aspects of the requirements for protection, and a substantial number of changes have been made to section 29.5.

(1) Express Statement on the Information

As the comments suggest, the ''information and records'' provided as PCII are occasionally not easily susceptible to labeling with an ''express statement.'' required for a proper submission. For that reason, the final rule provides for the use of a separate,

written ''express statement'' as set forth in paragraph (a)(3)(i).

(2) Oral Statements

Two comments were received regarding oral submissions during an ongoing crisis. These comments suggested that, where there might be many submissions, either the requirements for a written follow-up could be waived or PCII status could be assigned once and maintained throughout the crisis. DHS agrees with this suggestion and the rule has been changed to expand this capacity to the extent practical. The requirement for both an express statement and a certification statement has not been changed. However, the time in which these statements are required has been changed to ''a reasonable period'', as determined by the PCII Program Manager on a case-by-case basis, after CII submission, in whatever form. Further, DHS has added a section to make clear that electronic submissions are authorized and to establish appropriate procedures for such submissions.

(3) Certification Statement

Three commenters noted the requirement for a certification statement is not statutory. The certification statement is considered necessary, however, for effective program management and the rule continues to require a certification statement in paragraph (a)(4). The commenters suggested that there may be a public burden in submitting such a statement, and DHS has, in response, significantly simplified the submission requirements. The only information required in the certification statement is the submitter's contact information and any language considered necessary by the PCII Program Manager.

One commenter suggested that submitters be required to identify the steps that the submitter itself takes to protect the CII. The commenter suggested this information would assist the PCII Program Manager in determining a more appropriate and accurate determination of status. DHS has not adopted the suggestion.

One commenter suggested that the certification statement should be treated as PCII. The identifying information within the certification statement will be treated as PCII. Some substantive requirements of the certification statement have changed, however. The certification has been modified to incorporate provisions that the PCII Program Office has found necessary from an operating standpoint. For instance, PCII Program Office needs to know with whom it is dealing and how to contact responsible individuals. One commenter was concerned that unauthorized individuals might submit information on behalf of an entity, and suggested that, as a result, DHS establish parameters as to who is eligible to submit on behalf of an institution. DHS declines to do so. Even if parameters were established, there would be no practical way for DHS to determine whether the submitting individual is authorized by the entity to do so.

A commenter suggested DHS should provide forms for the PCII Program. Forms are not currently provided, and DHS does not believe that specific forms are needed. DHS has posted guidelines for submitters on the DHS Web site to assist potential submitters.

(4) Submission to the Program

The second sentence in paragraph (b) of the February 2004 Interim Rule relating to submissions to DHS components other than the Preparedness Directorate has been deleted as unnecessary. The PCII Program Manager or the Program Manager's designees should receive submittals of CII, as discussed above in Section II.A. This process effectively responds to a commenter that questioned the internal DHS receipt of CII.

Another commenter asked for special consideration for CII inadvertently submitted to the wrong agency or person. DHS believes its process is straightforward and further consideration for inadvertent submission is unnecessary. DHS will make available to potential submitters the means for submitting CII, and those means will be consistent with the protections of the Act.

A commenter suggested that it would be helpful if DHS could make advance determinations that any record falling within a certain class or category would be validated once and not every time a submission is made. As discussed below, DHS has added a new section 29.6(f) that addresses this issue and would be pleased to confer with any potential submitter regarding a possible submission.

F. Acknowledgment of Receipt, Validation, and Marking: Section 29.6

Section 29.6 was revised extensively in response to the comments received from the twelve commenters on this section and in light of operational decisions made by DHS.

(1) Presumption of Protection

Three commenters expressed their support for the presumption of protection afforded by this provision. To conform to the definition of PCII in section 29.2, new language clarifies that voluntarily submitted CII is PCII when submitted with an *express statement* even if the certification statement required by section 29.5(a)(4) is not initially received. *See also* section 29.6(d). If the information is deficient, the PCII Program Manager will attempt to contact the submitter to afford the submitter an opportunity to rectify the error or withdraw the submission and may properly label the submission him or herself.

(2) Marking

One commenter suggested that submitters be required to mark portions of submissions. DHS does not agree for reasons articulated elsewhere.

In response to another comment, language has been added to the marking statement contained in paragraph (c) to highlight the criminal and administrative penalties that could result from unauthorized release. This statement was omitted from the February 2004 Interim Rule provision.

The last sentence of marking statement included in paragraph (c) addresses what could otherwise be an alternative interpretation based on a literal reading that the regulation requires the submitter to maintain the submitted information in accordance with the procedures and requirements established by DHS rather than in accordance with its own procedures. That is not intended.

(3) Acknowledgement

A change to paragraph (d) adjusts the February 2004 Interim Rule statement regarding what is required before a submission receives the presumption of protection. Since submitted information need only be accompanied by an ''express statement'' in order to enjoy the presumption of protection, it is unnecessary to provide a certification before the PCII Program Manager or the PCII Program Manager's designee acknowledges receipt and takes action.

(4) Determinations of Non-Protected Status

Nine commenters addressed the handling and disposition of information that is found ineligible for protection under the CII Act, proposing the required destruction or the required return of the information; compliance with the submitter's instructions; or assurance that the information will continue to be treated confidentially and withheld from disclosure under the FOIA. As stated in the preamble to the February 2004 Interim Rule, DHS will

return submissions in almost all cases when it does not qualify as PCII.

The added words, ''within thirty calendar days of making a final determination,'' provide a new time limit for disposition of non-validated CII submissions, which is consistent with the period employed in the last sentence of the subparagraph. The 30-day period will run from the date of the notification rather than from the date of receipt of the notification by the submitter. The changes also supply a step previously missing from the language in the February 2004 Interim Rule regarding this provision, *i.e.*, that the PCII Program Office will make the initial determination final.

A commenter suggested that a 30-day time period for the Program Office to acknowledge receipt of a PCII submission was excessive; another requested the establishment of a time period to complete the validation process. Neither suggestion will be adopted. The volume of submissions is unpredictable, and 30 days to acknowledge receipt is a reasonable period. Recognizing the importance of timeliness, the PCII Program Manager will ensure that all processing is efficiently performed.

While notification to the submitter may, at the PCII Program Office's option, contain an explanation of why submitted information is not considered to be PCII under paragraph (e)(2)(ii), DHS does not accept the suggestion of two commenters that such an explanation be made obligatory. Additionally, paragraph (e)(2)(i)(A) has been modified to reflect the possible need to ask the submitter to provide the statement called for by section 29.5(a)(4), or any of the certifications that the statement is required to include, in order to perfect a submission.

Further, a new paragraph has been added at section 29.6 to allow for ''categorical inclusions'' in response to comments. This provision clarifies the Program Manager's authority to establish categories of information for which PCII status will automatically apply without a separate act of validation by the PCII Program Office.

(5) Changes From Protected to Non-Protected Status

Changes to paragraph (g) regarding a change in status from protected to non-protected are explained above in Section II. In response to a comment, this section has also been changed to specify that the procedures in paragraph (e)(2) of this section will be used prior to final determination of a change of status. As stated in the discussion of section 29.3(b) above, proposals that DHS either continuously review or establish a fixed schedule for regularly reviewing all PCII have been rejected.

G. Safeguarding of PCII: Section 29.7

Nine commenters addressed safeguarding issues in section 29.7, and two changes were made. In paragraph (b), the phrase ''in accordance with procedures prescribed by the PCII Program Manager'' was added in response to several comments asking for greater specificity in procedures for use and storage. The second change deletes a phrase in the February 2004 Interim Rule at the end of the paragraph that three commenters interpreted as giving the PCII Program Manager the discretion to establish ''tiered'' levels of security.

One commenter asked for a definition of ''official duties'' as that term is used in paragraph (c) regarding reproduction of PCII. Because the recipients of PCII are diverse, no general definition of ''official duties'' applicable to all is appropriate.

Two commenters believed paragraph (d) should specify that disposal should be in accordance with the Federal Records Act, 44 U.S.C. 3301. This section applies to Federal as well as other entities and DHS believes that requiring non-Federal entities to adhere to the Federal Records Act would be unnecessarily burdensome.

Two commenters suggested that paragraph (f) require transmission by secure *and encrypted* means. Another commenter asked for examples of what might be considered secure means. The PCII Program Manager will, as the rule states, determine the method of secure transmission. The method of transmission will not be the same in all cases. Encryption may be practical in some cases but not in others.

H. Disclosure of PCII: Section 29.8

This section was revised extensively based on comments received from sixteen commenters and on the operating experience of the PCII Program Office.

In response to two comments, a clarifying cross-reference in paragraph (a) was inserted in order to avoid giving this subsection an unintended legal effect that renders the subsequent provisions superfluous. Other language was deleted from this provision in the February 2004 Interim Rule because it was duplicative.

Four commenters proposed the involvement of submitters in DHS' information sharing decisions. DHS has not accepted these suggestions. Another commenter's objection to provisions requiring the submitter's consent to further disclosures of PCII likewise was rejected. DHS must make disclosure decisions based in the interests of the United States as a whole, including the interests of the submitters and the specific reasons and events that may warrant disclosure.

DHS is clarifying the distinction in paragraph (b) between how PCII may be used by the Federal government, and how it may be used by State, local, and tribal agencies. The CII Act limits the purposes for which State, local and tribal governments may use PCII and how State, local and tribal governments may share PCII. According to sections 214(a)(1)(E)(ii) and (iii) of the CII Act (6 U.S.C. 133(a)(1)(E)(ii) and (iii)), PCII may not be used by those governments for purposes other than protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act, and an agency of those governments may not further disclose the information without the consent of the submitter. These limitations are echoed in paragraphs (d)(1) and (3) of the February 2004 Interim Rule. The revision of this subsection brings the State, local and tribal sharing provisions into conformity with the statute and the other related rule provisions. The final sentence alters the requirement that State, local and tribal government entities enter into written agreements with the PCII Program Manager, specifying that they must instead enter into arrangements with the PCII Program Manager. This change was made to promote flexibility and, in exigent circumstances, a speedy sharing of information.

In response to eight commenters who expressed concern over possible unauthorized State, local or tribal government disclosures of PCII that might be provided to them, or who urged the adoption of strict controls on the sharing of such information with State, local and tribal governments, these arrangements, except in exigent circumstances will be very specific, will require safeguarding, handling, violation reporting, and other procedures consistent with this rule, and will further provide for compliance monitoring. In most cases DHS anticipates that these arrangements will be in the form of a Memorandum of Agreement (MOA) that will also recognize the preeminence of PCII status under the CII Act and these regulations in relation to any State, territorial, or tribal public disclosure laws or policies. Further, DHS has added language that makes clear that PCII may not be used for regulatory purposes.

In paragraph (c), the first change clarifies that State, local and tribal

contractors can receive PCII under the same conditions as Federal contractors. As in the case of Federal contractors, State, local, and tribal contractors are agents of a governmental entity, carrying out the functions on behalf of the government in furtherance of its mission and under its direction. Therefore, DHS does not consider State, local and tribal contractors to be precluded from receiving PCII as ''any other party;'' rather, DHS considers them an extension of the State, local or tribal governmental entity.

The second change is to employ a term defined in section 29.2, to replace the subjective term, ''purposes of DHS'' with the term ''purposes of the CII Act.'' This change also better lends itself to PCII Program Office certifications of contractors to Federal agencies other than DHS. All contractor employees working on PCII Program matters and having access to PCII, rather than the more abstract ''identified category'' of employees, will be required to sign a nondisclosure agreement (NDA). Also added is a provision that the NDAs will be in a form prescribed by the PCII Program Manager. Based on PCII Program Office operating experience, reference to ''contractor'' signature of NDAs has been deleted; contractors will continue to be obliged to agree, by contract, to comply with all programmatic requirements.

Additionally, as discussed above in section II.C, a change was made to permit employees of Federal, State, local, and tribal contractors who are engaged in the performance of services in support of the purposes of the CII Act, to communicate with a submitting person or an authorized person of a submitting entity about their submittal or information when authorized by the PCII Program Manager or a PCII Program Manager's designee. The previous prohibition against disclosure to any of the contractors' components and the reference to ''additional employees'' posed an unnecessary operating difficulty for contractors, which was noted by one commenter. These provisions have been replaced by the more comprehensible but sufficiently strict prohibition on disclosing to ''any other party.'' This is the term used in section 29.8(d)(1), which prohibits State, local, and tribal governments from making disclosures to ''any other party not already authorized to receive such information.''

A commenter suggested that a PCII Officer certify the distribution of PCII to Federal contractors on a specific PCII case-by-case basis rather than based on a certification that the contractor was performing services on behalf of DHS. This suggestion will not be adopted. Such a requirement could be burdensome, and moreover, is unnecessary. PCII will only be distributed as required for the contractor's use. The single certification does not entitle the contractor to all PCII, but only PCII the governmental agency determines the contractor needs.

Another commenter asked for clarification of what type of language would constitute the authorization from the submitter to enable sharing of PCII. The relevant question is how DHS will ask for permission, and DHS envisions that the request will be in writing, state the tracking number previously provided to the submitter, identify the requester and the intended recipient, and ask for a response within a certain number of days.

Consistent with the changes discussed above, a change was made in paragraph (d)(1) to eliminate the idea that consent to further disclosure could be made by someone ''on whose behalf'' information was submitted.

A comment questioned the statement in the preamble to the February 2004 Interim Rule that State, local and tribal governments ''will be asked to track further disclosures'' and suggested the requirement to track should remain with DHS. As the comment noted, any further distribution by State, local, and tribal governments requires submitter permission, a process administratively handled by DHS. DHS will impose a tracking requirement on State, local and tribal governments and will also have its own records of permissions in the PCIIMS.

Changes in paragraph (e) of this section have been explained in detail in section II above. An additional change to paragraph (e) not discussed above is that the language now allows not only the Directorate for Preparedness, but also other Federal agencies, as well as State, local and tribal government entities, to use PCII in preparing advisories and similar communications. The list of things to be protected from disclosure has been rephrased in the disjunctive, correcting the unduly restrictive conjunctive phrasing, which was noted by one commenter. The final change adds language that permits Federal, State, local and tribal governmental entities to contact submitters directly to confer if there is a question about the PCII to be used in the advisory, alert, or warning.

A comment suggested that paragraph (f)(1)(i), which limits use or disclosure of PCII by Federal employees except as authorized, is important enough to warrant its own rule provision. The comment was considered; however, further changes were not deemed necessary. However, in reviewing the paragraph it is clear that sections of the CII Act other than 214(a)(1)(D) and (E) (6 U.S.C. 133(a)(1)(D), (E)), for example, were applicable to the general category of ''Exceptions for disclosure.'' The language in the subparagraph was therefore modified to make clear that it applied to entities and persons other than officers and employees of the United States.

Language was added to make paragraph (f)(1)(i)(A) consistent with the position that State, local, and tribal investigations or prosecutions should be coordinated by a Federal law enforcement official. It also recognizes that PCII could be used in furtherance of a foreign government investigation or prosecution, and imposes, for any disclosure to the foreign government, the same requirement for coordination by a Federal law enforcement official.

Paragraph (f)(1)(i)(C) has been limited to the disclosure of information by an officer or employee of the United States, as this paragraph fits clearly within the confines of section 214(a)(1)(D) of the CII Act (6 U.S.C. 133(a)(1)(D)).

Section (f)(3) of the 2004 Interim Final Rule referred to the Whistleblower Protection Act and has been omitted because is merely restates the law of the land. Section (f)(4) of the February 2004 Interim Rule has been deleted because it was deemed unnecessary.

DHS has modified the language in paragraph (g) to more accurately reflect the intention of the statutory language in section 214(a)(1)(E)(i) of the CII Act.

As discussed in Section II, paragraph (j) has been deleted in its entirety. Further, paragraph (k) has been deleted because it improperly rested sole authority to request submitter consent for further dissemination in the PCII Program Manager, thus limiting flexibility and effectiveness, especially in exigent circumstances.

I. Investigation and Reporting of Violation of PCII Procedures: Section 29.9

Six comments expressed concern that there were no provisions for the imposition of penalties or sanctions on State, local and tribal government employees or on contractors. The provisions of subsection (d) reflect the language of section 214(f) of the CII Act (6 U.S.C. 133(f)). This section applies unambiguously only to officers and employees of the United States. DHS has no authority to make these provisions applicable to anyone else. However, DHS will place in the MOAs for State, local and tribal governments, when used, or when an arrangement

other than an MOA is used, then to the extent practicable, language that will require the State, local, or tribal government to consider breaches of the agreements by employees as matters subject to the criminal code or to the applicable employee code of conduct for that jurisdiction. While States do not have laws that were written specifically with PCII in mind, they do have laws that govern theft, conspiracy, trade secrets, and the like, which could apply to employees and to contractors as well. The CII Act does not limit any other enforcement mechanism; the CII Act adds a specific criminal enforcement provision applicable to Federal employees.

A commenter suggested that this section should specifically require that the DHS Inspector General, the PCII Program Manager, or the Preparedness Security Officer investigate unauthorized disclosures by State, local and tribal governments. As previously noted, the relevant MOAs or alternative arrangements will generally provide for DHS to monitor all State, local and tribal governments with respect to their compliance with the guidance regarding handling PCII.

A commenter asked whether DHS had considered the applicability of the Privacy Act of 1974, 5 U.S.C. 552a, to any part of the submissions process. DHS has considered and continues to consider the interrelationship between the CII Act and the Privacy Act, and, through the Program Office and the DHS Privacy Officer, will ensure that the PCII program conducts all activities related to the PCII Program in conformance with the Privacy Act.

IV. Revision of Part 29

After considering all of the comments and the changes warranted, DHS determined that the entire part should be revised rather then making individual amendments to the specific sections and paragraphs. Individual amendments to each section and paragraph would have created a very large number of instructions to the **Federal Register** and rendered the amended regulation difficult, if not impossible, to understand without reading the amendments side-by-side with the current regulations. Accordingly, DHS has repromulgated all of the provisions of part 29, whether amended by this final rule or as in the February 2004 Interim Rule, to assist the reader.

V. Consideration of Various Laws and Executive Orders

A. Administrative Procedure Act

DHS has determined that good cause exists to make this regulation effective upon publication in the **Federal Register** under 5 U.S.C. 553(d)(3). This final rule clarifies ambiguities in the February 2004 Interim Rule that were identified by the public comments and has the advantage of taking into consideration operating experience with submitters gained since the February 2004 Interim Rule became effective on February 20, 2004. DHS believes that submitters are more likely to provide information that qualifies for protection under the CII Act of 2002 when the final rule goes into effect. Such PCII would help DHS implement security measures and issue warnings. After considering the likelihood that valuable information is now being withheld because of concern and confusion as to how it might be handled under the February 2004 Interim Rule, and the possibility that this information could be useful in deterring or responding to a security incident, the Department has concluded that good cause exists for making the regulation effective immediately.

B. Executive Order 12866 Assessment

DHS is required to implement this rule under the Critical Infrastructure Information Act of 2002, Title II, Subtitle B, of the Homeland Security Act of 2002 (6 U.S.C. 211 *et seq.*). This rule is considered by DHS to be a significant regulatory action under Executive Order 12866, 58 FR 51735 (Oct. 4, 1993), Regulatory Planning and Review, section 3(f). Accordingly, this regulation has been submitted to the Office of Management and Budget (OMB) for review.

DHS has performed an analysis of the expected costs and benefits of this final rule. A similar analysis was performed before the February 2004 Interim Rule was made effective. This new analysis considers comments received regarding staff costs and storage assumptions. Consideration of these comments does not change the previous conclusions.

The final rule affects persons and entities in the private sector that have CII they wish to share with DHS. The final rule also affects State, local and tribal governments with which DHS has signed agreements detailing the procedures on how PCII must be safeguarded, used, and destroyed when it is no longer needed.

Private sector submitters of CII must determine first whether to participate and if so, develop and follow internal procedures for submissions that comply with this regulation. Recipients of PCII must follow the procedures established in this regulation and as specified in agreements with the PCII Program Manager.

Costs

DHS believes private entities that submit CII will not incur significant costs. For submitters of CII other than individuals, there will likely be a one-time decision process to determine whether participation is appropriate, and if so, the establishment of internal operating procedures. A legal review of those submitters' procedures would likely be undertaken internally to ensure that they result in submissions that will receive the protections of the CII Act. The costs to develop the procedures would be a non-recurring expense and it is unlikely that a separate legal review would be required for each submission. Individuals who might want to submit CII will probably read the applicable procedures posted on the DHS Web site and have no non-recurring costs. Recurring expenses for submitting entities could include the cost of transmitting the CII, office supplies, costs associated with internal marking of retained copies of CII, and the expense of making available a point of contact with DHS to discuss the entity's submission. The non-recurring costs described will be different for each entity and also depend on how frequently submissions are made, but it is unlikely an entity will be required to increase its workforce. The costs are expected to be only a slight increment to ongoing total costs and managerially insignificant, perhaps even unidentifiable.

Costs for State, local and tribal governments that are the recipients of PCII will include the appointment of a PCII Officer to ensure safeguarding and destruction in accordance with these procedures and in the required written agreements. The position of PCII Officer for State, local, and tribal governments is not anticipated to be a full time position, although it could be. Should the position evolve into a full time one for a State, the costs should not exceed $150,000 per year per State. In the unlikely event all 50 States had full time PCII Officers, these costs would be approximately $7,500,000 per year. These costs are based on DHS estimates based on equivalent Federal positions and costs. A PCII Officer will be required to become familiar with procedures and be responsible for the training of others. DHS will develop training material and provide trainers for this effort. DHS anticipates that States will, to a large extent, appoint a

PCII Officer whose responsibilities will include overseeing local and tribal government participation. Thus, in most cases it will not be necessary for local and tribal governments to appoint PCII Officers. DHS believes that the costs to State, local and tribal governments other than those associated with PCII Officers will include storage capabilities, supplies, general overhead expenses and record keeping systems. These costs are variable and will depend on the volume of PCII received. The total of these costs is not expected to be significant.

Benefits

This program will permit the private sector to provide CII to DHS with confidence that it will not be inappropriately released to the public. The expected benefit of this program is centralized knowledge of the country's critical infrastructure everyone uses to conduct the daily affairs of life. As noted above, 85% of critical infrastructure is not possessed by the United States Government. Destruction of this infrastructure, or interruptions in its operating capability, could be catastrophic. With such knowledge comes the ability to issue warnings, to conduct analyses of systemic weaknesses, and to take actions to prevent terrorist acts. If the information provided results in but one thwarted terrorist act, or perhaps deters even the attempt, the benefit has been realized. Monetarily, the benefit might be calculated as the avoidance of the reconstruction cost of the facility damaged and the loss in commercial activity attributable to the lost facility. Not all the benefits of this regulation can be easily quantified as the benefits of this rule include preventing a terrorist event and the probability and consequences from that event are extremely difficult to predict. Given the relatively small implementation costs, DHS believes the potential benefits outweigh costs by a large margin.

C. Regulatory Flexibility Act

The Regulatory Flexibility Act (5 U.S.C. 601 *et seq.*) (RFA) requires an agency to review regulations to assess their impact on small entities. An agency must conduct a regulatory flexibility analysis unless it determines and certifies that a rule is not expected to have a significant impact on a substantial number of small entities. DHS has reviewed this final rule and, by approving it, certifies that this rule will not have a significant economic impact on a substantial number of small entities.

Many of the entities expected to voluntarily submit CII to DHS will be providers of infrastructure and protected systems. Typically, infrastructure providers are large public utilities or companies and providers of protected systems are large companies that will not meet the definition of small businesses for purposes of the RFA. It is possible that small non-profit organizations or any other small entities that provide critical infrastructure, such as telephone or electric cooperatives, might from time to time provide CII. The costs to send the CII to DHS are expected to be small and depend in large measure on the frequency of submissions. It is unlikely that a small utility cooperative, or any other small entities, will send CII on any ongoing basis, and hence any costs will not have a significant impact on any organization that chooses to participate. Small governmental jurisdictions are expected to depend on the State government for warnings and analysis and generally not appoint PCII Officers or establish separate programs. Those small jurisdictions will likely be only receivers, not providers, of information that is produced and distributed by the PCII Program Office and this rule will have no significant impact.

D. Unfunded Mandates Reform Act of 1995

This rule will not result in the expenditure by State, local and tribal governments, in the aggregate, or by the private sector, of $100 million or more (adjusted annually for inflation) in any one year, and it will not significantly or uniquely affect small governments. Therefore, no actions were deemed necessary under the provisions of the Unfunded Mandates Reform Act of 1995.

E. Small Business Regulatory Enforcement Act of 1996

This rule is not a major rule, as defined by section 804 of the Small Business Regulatory Enforcement Act of 1996. This rule will not result in an annual effect on the United States economy of $100 million or more, result in a major increase in costs or prices, or significant adverse effects on competition, employment, investment, productivity, innovation, or on the ability of United States-based companies to compete with foreign-based companies in domestic and export markets.

F. Executive Order 13132—Federalism

The preamble to the February 2004 Interim Rule requested comment on the federalism impact of the February 2004 Interim Rule. No comments were received.

This final rule was analyzed in accordance with the principles and criteria contained in Executive Order 13132 (''Federalism''). This rulemaking, as required by the underlying statute, preempts State, local and tribal laws that might otherwise require disclosure of PCII and precludes use of PCII in certain State civil actions unless permission of the submitter is obtained. This preemption is expected to inure to the benefit of the States by making it possible for PCII that is provided to the Federal Government to be shared with the States. The rule does not impose any regulation that has substantial direct effects on the States, the relationship between the national government and the States, or the distribution of power and responsibilities among the various levels of government. Therefore, the consultation requirements of Executive Order 13132 do not apply.

G. Executive Order 12988—Civil Justice Reform

This rule meets the applicable standards set forth in sections 3(a) and 3(b)(2) of Executive Order 12988.

H. Paperwork Reduction Act of 1995

Under the Paperwork Reduction Act of 1995, 44 U.S.C. 3501–3520 (PRA), a Federal agency must obtain approval from the OMB for each collection of information it conducts, sponsors, or requires through regulations. This rule does not contain provisions for collection of information, does not meet the definition of ''information collection'' as defined under 5 CFR part 1320, and is therefore exempt from the requirements of the PRA. Accordingly, there is no requirement to obtain OMB approval for information collection.

I. Environmental Analysis

DHS has analyzed this regulation for purposes of the National Environmental Policy Act and has concluded that this rule will not have any significant impact on the quality of the human environment.

List of Subjects in 6 CFR Part 29

Confidential business information, Reporting and recordkeeping requirements.

Authority and Issuance

■ For the reasons discussed in the preamble, 6 CFR part 29 is revised to read as follows:

PART 29—PROTECTED 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 of this Part.* This Part implements sections 211 through 215 of the Homeland Security Act of 2002 (HSA) through the establishment of uniform procedures for the receipt, care, and storage of Critical Infrastructure Information (CII) voluntarily submitted to the Department of Homeland Security (DHS). Title II, Subtitle B, of the Homeland Security Act is referred to herein as the Critical Infrastructure Information Act of 2002 (CII Act). Consistent with the statutory mission of DHS to prevent terrorist attacks within the United States and reduce the vulnerability of the United States to terrorism, DHS will encourage the voluntary submission of CII by safeguarding and protecting that information from unauthorized disclosure and by ensuring that such information is, as necessary, securely shared with State and local government pursuant to section 214(a) through (g) of the CII Act. As required by the CII Act, these rules establish procedures regarding:

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

(2) The receipt, validation, handling, storage, proper marking and use of information as PCII;

(3) The safeguarding and maintenance of the confidentiality of such information, appropriate sharing of such information with State and local governments pursuant to section 214(a) through (g) of the HSA.

(4) The issuance of advisories, notices and warnings related to the protection of critical infrastructure or protected systems in such a manner as to protect from unauthorized disclosure the source of critical infrastructure information that forms the basis of the warning, and any information that is proprietary or business sensitive, might be used to identify the submitting person or entity, or is otherwise not appropriately in the public domain.

(b) *Scope.* The regulations in this Part apply to all persons and entities that are authorized to handle, use, or store PCII or that otherwise accept receipt of PCII.

§ 29.2 Definitions.

For purposes of this part:

(a) *Critical Infrastructure* has the meaning stated in section 2 of the Homeland Security Act of 2002 (referencing the term used in section 1016(e) of Public Law 107–56 (42 U.S.C. 5195c(e)).

(b) *Critical Infrastructure Information*, or *CII*, has the same meaning as established in section 212 of the CII Act of 2002 and means information not customarily in the public domain and related to the security of critical infrastructure or protected systems, including documents, records or other 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, local, or tribal law, harms 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) *Information Sharing and Analysis Organization*, or *ISAO*, has the same meaning as is established in section 212 of the CII Act of 2002 and 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, so as to ensure the availability, integrity, and reliability thereof;

(2) Communicating or disclosing CII 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 CII 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 (c)(1) and (2) of this section.

(d) *In the public domain* means information lawfully, properly and regularly disclosed generally or broadly to the public. Information regarding system, facility or operational security is not ''in the public domain.'' Information submitted with CII that is proprietary or business sensitive, or which might be used to identify a submitting person or entity will not be considered ''in the public domain.'' Information may be ''business sensitive'' for this purpose whether or not it is commercial in nature, and even if its release could not demonstrably cause substantial harm to the competitive position of the submitting person or entity.

(e) *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 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) *Program Manager's Designee* means a Federal employee outside of the PCII Program Office, whether employed by DHS or another Federal agency, to whom certain functions of the PCII Program Office are delegated by the Program Manager, as determined on a case-by-case basis.

(g) *Protected Critical Infrastructure Information*, or *PCII*, means validated CII, including information covered by 6 CFR 29.6(b) and (f), including the identity of the submitting person or entity and any person or entity on whose behalf the submitting person or entity submits the CII, that is voluntarily submitted, directly or indirectly, to DHS, for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other appropriate

purpose, and any information, statements, compilations or other materials reasonably necessary to explain the CII, put the CII in context, describe the importance or use of the CII, when accompanied by an express statement as described in 6 CFR 29.5.

(h) *Protected Critical Infrastructure Information Program*, or *PCII Program*, means the program implementing the CII Act, including the maintenance, management, and review of the information provided in furtherance of the protections provided by the CII Act.

(i) *Protected system* has the meaning set forth in section 212(6) of the CII Act, and 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.

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

(k) *Regulatory proceeding*, as used in Section 212(7) of the CII Act and these rules, means administrative proceedings in which DHS is the adjudicating entity, and does not include any form or type of regulatory proceeding or other matter outside of DHS.

(l) *State* has the same meaning set forth in section 2 of the Homeland Security Act of 2002 and means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States.

(m) *Submission* as referenced in these procedures means any transmittal, either directly or indirectly, of CII to the DHS PCII Program Manager or the PCII Program Manager's designee, as set forth herein.

(n) *Submitted in good faith* means any submission of information that could reasonably be defined as CII or PCII under this section. Upon validation of a submission as PCII, DHS has conclusively established the good faith of the submission. Any information qualifying as PCII by virtue of a categorical inclusion identified by the Program Manager pursuant to section 214 of the CII Act and this Part is submitted in good faith.

(o) *Voluntary* or *voluntarily*, when used in reference to any submission of CII, means the submittal thereof in the absence of an exercise of legal authority by DHS to compel access to or submission of such information. Voluntary submission of CII may be accomplished by (*i.e.*, come from) a single state or local governmental entity; private entity or person; or by an ISAO acting on behalf of its members or otherwise. There are two exclusions from this definition. 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'' or ''voluntarily'' 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 U.S. Securities and Exchange Commission or with Federal banking regulators or a writing that accompanied the solicitation of an offer or a sale of securities. Information or statements previously submitted to DHS in the course of a regulatory proceeding or a licensing or permitting determination are not ''voluntarily submitted.'' In addition, the submission of information to DHS for purposes of seeking a Federal preference or benefit, including CII submitted to support an application for a DHS grant to secure critical infrastructure will be considered a voluntary submission of information. Applications for SAFETY Act Designation or Certification under 6 CFR Part 25 will also be considered a voluntary submission.

(p) The term *used directly by such agency, any other Federal, State, or local authority, or any third party, in any civil action arising under Federal or State law* in section 214(a)(1)(C) of the CII Act means any use in any proceeding other than a criminal prosecution before any court of the United States or of a State or otherwise, of any PCII, or any drafts or copies of PCII retained by the submitter, including the opinions, evaluations, analyses and conclusions prepared and submitted as CII, as evidence at trial or in any pretrial or other discovery, notwithstanding whether the United States, its agencies, officers, or employees is or are a party to such proceeding.

§ 29.3 Effect of provisions.

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

(b) *Restriction on use of PCII by regulatory and other Federal, State, and Local agencies.* A Federal, State or local agency that receives PCII may utilize the PCII only for purposes appropriate under the CII Act, including securing critical infrastructure or protected systems. Such PCII may not be utilized for any other collateral regulatory purposes without the written consent of the PCII Program Manager and of the submitting person or entity. The PCII Program Manager or the PCII Program Manager's designee shall not share PCII with Federal, State or local government agencies without instituting appropriate measures to ensure that PCII is used only for appropriate purposes.

§ 29.4 Protected Critical Infrastructure Information Program administration.

(a) *Preparedness Directorate Program Management.* The Secretary of Homeland Security hereby designates the Under Secretary for Preparedness as the senior DHS official responsible for the direction and administration of the PCII Program. He shall administer this program through the Assistant Secretary for Infrastructure Protection.

(b) *Appointment of a PCII Program Manager.* The Under Secretary for Preparedness shall:

(1) Appoint a PCII Program Manager serving under the Assistant Secretary for Infrastructure Protection who is responsible for the administration of the PCII Program;

(2) Commit resources necessary for the effective implementation of the PCII 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 PCII Program to facilitate secure information sharing with appropriate authorities.

(4) Promulgate implementing directives and prepare training materials as ppropriate for the proper treatment of PCII.

(c) *Appointment of PCII Officers.* The PCII Program Manager shall establish procedures to ensure that each DHS component and each Federal, State, or local entity that works with PCII appoint one or more employees to serve as a PCII Officer in order to carry out the responsibilities stated in paragraph (d)

of this section. Persons appointed to serve as PCII Officers shall be fully familiar with these procedures.

(d) *Responsibilities of PCII Officers.* PCII Officers shall:

(1) Oversee the handling, use, and storage of PCII;

(2) Ensure the secure sharing of PCII with appropriate authorities and individuals, as set forth in 6 CFR 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 compliance with handling, use, and storage of PCII;

(4) Establish additional procedures, measures and penalties as necessary to prevent unauthorized access to PCII; and

(5) Ensure prompt and appropriate coordination with the PCII Program Manager regarding any request, challenge, or complaint arising out of the implementation of these regulations.

(e) *Protected Critical Infrastructure Information Management System (PCIIMS).* The PCII Program Manager shall develop, for use by the PCII Program Manager and the PCII Manager's designees, 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 PCII. This compilation of PCII shall be safeguarded and protected in accordance with the provisions of the CII Act. The PCII Program Manager may require the completion of appropriate background investigations of an individual before granting that individual access to any PCII.

§ 29.5 Requirements for protection.

(a) CII shall receive the protections of section 214 of the CII Act when:

(1) Such information is voluntarily submitted, directly or indirectly, to the PCII Program Manager or the PCII Program Manager's designee;

(2) The information is submitted for protected use regarding the security of critical infrastructure or protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other appropriate purposes including, without limitation, for the identification, analysis, prevention, preemption, disruption, defense against and/or mitigation of terrorist threats to the homeland;

(3) The information is labeled with an express statement as follows:

(i) In the case of documentary submissions, 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:

(A) Through an oral statement, made at the time of the oral submission or within a reasonable period thereafter, indicating an expectation of protection from disclosure as provided by the provisions of the CII Act; and

(B) Through a written statement substantially similar to the one specified above accompanied by a document that memorializes the nature of oral information initially provided received by the PCII Program Manager or the PCII Program Manager's designee within a reasonable period after using oral submission; and

(iii) In the case of electronic information:

(A) Through an electronically submitted statement within a reasonable period of the electronic submission indicating an expectation of protection from disclosure as provided by the provisions of the CII Act; and

(B) Through a non-electronically submitted written statement substantially similar to the one specified above accompanied by a document that memorializes the nature of e-mailed information initially provided, to be received by the PCII Program Manager or the PCII Program Manager's designee within a reasonable period after using e-mail submission.

(4) The submitted information additionally is accompanied by a statement, signed by the submitting person or an authorized person on behalf of an entity identifying the submitting person or entity, containing such contact information as is considered necessary by the PCII Program Manager, and certifying that the information being submitted is not customarily in the public domain;

(b) Information that is not submitted to the PCII Program Manager or the PCII Program Manager's designees will not qualify for protection under the CII Act. Only the PCII Program Manager or the PCII Program Manager's designees are authorized to acknowledge receipt of information being submitted for consideration of protection under the Act.

(c) All Federal, State and local government entities shall protect and maintain information as required by these rules or by the provisions of the CII Act when that information is provided to the entity by the PCII Program Manager or the PCII Program Manager's designee and is marked as required in 6 CFR 29.6(c).

(d) All submissions seeking PCII status shall be presumed to have been submitted in good faith until validation or a determination not to validate pursuant to these rules.

§ 29.6 Acknowledgment of receipt, validation, and marking.

(a) *Authorized officials.* Only the DHS PCII Program Manager is authorized to validate, and mark information as PCII. The PCII Program Manager or the Program Manager's designees, may mark information qualifying under categorical inclusions pursuant to 6 CFR 29.6(f).

(b) *Presumption of protection.* All information submitted in accordance with the procedures set forth hereby will be presumed to be and will be treated as PCII, enjoying the protections of section 214 of the CII Act, from the time the information is received by the PCII Program Office or the PCII Program Manager's designee. The information shall remain protected unless and until the PCII Program Office renders a final decision that the information is not PCII. The PCII Program Office will, with respect to information that is not properly submitted, inform the submitting person or entity within thirty days of receipt, by a means of communication to be prescribed by the PCII Program Manager, that the submittal was procedurally defective. The submitter will then have an additional 30 days to remedy the deficiency from receipt of such notice. If the submitting person or entity does not cure the deficiency within thirty calendar days of the date of receipt of the notification provided in this paragraph, the PCII Program Office may determine that the presumption of protection is terminated. Under such circumstances, the PCII Program Office may cure the deficiency by labeling the submission with the information required in 6 CFR 29.5 or may notify the applicant that the submission does not qualify as PCII. No CII submission will lose its presumptive status as PCII except as provided in 6 CFR 29.6(g).

(c) *Marking of information.* All PCII shall be clearly identified through markings made by the PCII Program Office. The PCII Program Office shall mark PCII materials as follows: ''This document contains PCII. In accordance with the provisions of 6 CFR Part 29, this document is exempt from release under the Freedom of Information Act (5 U.S.C. 552(b)(3)) and similar laws requiring public disclosure. Unauthorized release may result in criminal and administrative penalties. This document is to be safeguarded and

disseminated in accordance with the CII Act and the PCII Program requirements.'' When distributing PCII, the distributing person shall ensure that the distributed information contains this marking.

(d) *Acknowledgement of receipt of information.* The PCII Program Office or the PCII Program Manager's designees shall acknowledge receipt of information submitted as CII and accompanied by an express statement, and in so doing shall:

(1) Contact the submitting person or entity, within thirty calendar days of receipt of the submission of CII, by the means of delivery prescribed in procedures developed by the PCII Program Manager. In the case of oral submissions, receipt will be acknowledged in writing within thirty calendar days after receipt by the PCII Program Office or the PCII Program Manager's designee of a written statement, certification, and documents that memorialize the oral submission, as referenced in 6 CFR 29.5(a)(3)(ii);

(2) Enter the appropriate data into the PCIIMS as required in 6 CFR 29.4(e); and

(3) Provide the submitting person or entity with a unique tracking number that will accompany the information from the time it is received by the PCII Program Office or the PCII Program Manager's designees.

(e) *Validation of information.* (1) The PCII Program Manager shall be responsible for reviewing all submissions that request protection under the CII Act. The PCII Program Manager shall review the submitted information as soon as practicable. If a final determination is made that the submitted information meets the requirements for protection, the PCII Program Manager shall ensure that the information has been marked as required in paragraph (c) of this section, notify the submitting person or entity of the determination, and disclose it only pursuant to 6 CFR 29.8.

(2) If the PCII Program Office makes an initial determination that the information submitted does not meet the requirements for protection under the CII Act, the PCII Program Office shall:

(i) Notify the submitting person or entity of the initial determination that the information is not considered to be PCII. This notification also shall, as necessary:

(A) Request that the submitting person or entity complete the requirements of 6 CFR 29.5(a)(4) or further explain the nature of the information and the submitting person or entity's basis for believing the information qualifies for protection under the CII Act;

(B) Advise the submitting person or entity that the PCII Program Office will review any further information provided before rendering a final determination;

(C) Advise the submitting person or entity that the submission can be withdrawn at any time before a final determination is made;

(D) Notify the submitting person or entity that until a final determination is made the submission will be treated as PCII;

(E) Notify the submitting person or entity that any response to the notification must be received by the PCII Program Office no later than thirty calendar days after the date of the notification; and

(F) Request the submitting person or entity to state whether, in the event the PCII Program Office makes a final determination that any such information is not PCII, the submitting person or entity prefers that the information be maintained without the protections of the CII Act or returned to the submitter or destroyed. If a request for withdrawal is made, all such information shall be returned to the submitting person or entity.

(ii) If the information submitted has not been withdrawn by the submitting person or entity, and the PCII Program Office, after following the procedures set forth in paragraph (e)(2)(i) of this section, makes a final determination that the information is not PCII, the PCII Program Office, in accordance with the submitting person or entity's written preference, shall, within thirty calendar days of making a final determination, return the information to the submitter. If return to the submitter is impractical, the PCII Program Office shall destroy the information within 30 days. This process is consistent with the appropriate National Archives and Records Administration-approved records disposition schedule. If the submitting person or entity cannot be notified or the submitting person or entity's response is not received within thirty calendar days of the date of the notification as provided in paragraph (e)(2)(i) of this section, the PCII Program Office shall make the initial determination final and return the information to the submitter.

(f) *Categorical Inclusions of Certain Types of Infrastructure as PCII.* The PCII Program Manager has discretion to declare certain subject matter or types of information categorically protected as PCII and to set procedures for receipt and processing of such information. Information within a categorical inclusion will be considered validated upon receipt by the Program Office or any of the Program Manager's designees without further review, provided that the submitter provides the express statement required by section 214(a)(1). Designees shall provide to the Program Manager information submitted under a categorical inclusion.

(g) *Changing the status of PCII to non-PCII.* Once information is validated, only the PCII Program Office may change the status of PCII to that of non-PCII and remove its PCII markings. Status changes may only take place when the submitting person or entity requests in writing that the information no longer be protected under the CII Act; or when the PCII Program Office determines that the information was, at the time of the submission, customarily in the public domain. Upon making an initial determination that a change in status may be warranted, but prior to a final determination, the PCII Program Office, using the procedures in paragraph (e)(2) of this section, shall inform the submitting person or entity of the initial determination of a change in status. Notice of the final change in status of PCII shall be provided to all recipients of that PCII under 6 CFR 29.8.

§ 29.7 Safeguarding of Protected Critical Infrastructure Information.

(a) *Safeguarding.* All persons granted access to PCII are responsible for safeguarding such information in their possession or control. PCII shall be protected at all times by appropriate storage and handling. Each person who works with PCII is personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to it.

(b) *Background Checks on Persons with Access to PCII.* For those who require access to PCII, DHS will, to the extent practicable and consistent with the purposes of the Act, undertake appropriate background checks to ensure that individuals with access to PCII do not pose a threat to national security. These checks may also be waived in exigent circumstances.

(c) *Use and Storage.* When PCII is in the physical possession of a person, reasonable steps shall be taken, in accordance with procedures prescribed by the PCII Program Manager, to minimize the risk of access to PCII by unauthorized persons. When PCII is not in the physical possession of a person, it shall be stored in a secure environment.

(d) *Reproduction.* Pursuant to procedures prescribed by the PCII 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.

(e) *Disposal of information.* Documents and material containing PCII may be disposed of by any method that prevents unauthorized retrieval, such as shredding or incineration.

(f) *Transmission of information.* PCII shall be transmitted only by secure means of delivery as determined by the PCII Program Manager, and in conformance with appropriate federal standards.

(g) *Automated Information Systems.* The PCII Program Manager shall establish security requirements designed to protect information to the maximum extent practicable, and consistent with the Act, for Automated Information Systems that contain PCII. Such security requirements will be in conformance with the information technology security requirements in the Federal Information Security Management Act and the Office of Management and Budget's implementing policies.

§ 29.8 Disclosure of Protected Critical Infrastructure Information.

(a) *Authorization of access.* The Under Secretary for Preparedness, the Assistant Secretary for Infrastructure Protection, or either's designee may choose to provide or authorize access to PCII under one or more of the subsections below when it is determined that this access supports a lawful and authorized government purpose as enumerated in the CII Act or other law, regulation, or legal authority.

(b) *Federal, State and Local government sharing.* The PCII Program Manager or the PCII Program Manager's designees may provide PCII to an employee of the Federal government, provided, subject to subsection (f) of this section, that such information is shared for purposes of securing the critical infrastructure or protected systems, analysis, warning, interdependency study, recovery, reconstitution, or for another appropriate purpose including, without limitation, the identification, analysis, prevention, preemption, and/or disruption of terrorist threats to the homeland. PCII may not be used, directly or indirectly, for any collateral regulatory purpose. PCII may be provided to a State or local government entity for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act. The provision of PCII to a State or local government entity will normally be made only pursuant to an arrangement with the PCII Program Manager providing for compliance with the requirements of paragraph (d) of this section and acknowledging the understanding and responsibilities of the recipient. State and local governments receiving such information will acknowledge in such arrangements the primacy of PCII protections under the CII Act; agree to assert all available legal defenses to disclosure of PCII under State, or local public disclosure laws, statutes or ordinances; and will agree to treat breaches of the agreements by their employees or contractors as matters subject to the criminal code or to the applicable employee code of conduct for the jurisdiction.

(c) *Disclosure of information to Federal, State and local government contractors.* Disclosure of PCII to Federal, State, and local contractors may be made when necessary for an appropriate purpose under the CII Act, and only after the PCII Program Manager or a PCII Officer certifies that the contractor is performing services in support of the purposes of the CII Act. The contractor's employees who will be handling PCII must sign individual nondisclosure agreements in a form prescribed by the PCII Program Manager, and the contractor must agree by contract, whenever and to whatever extent possible, to comply with all relevant requirements of the PCII Program. The contractor shall safeguard PCII in accordance with these procedures and shall not remove any ''PCII'' markings. An employee of the contractor may, in the performance of services in support of the purposes of the CII Act and when authorized to do so by the PCII Program Manager or the PCII Program Manager's designee, communicate with a submitting person or an authorized person of a submitting entity, about a submittal of information by that person or entity. Contractors shall not further disclose PCII to any other party not already authorized to receive such information by the PCII Program Manager or PCII Program Manager's Designee, without the prior written approval of the PCII Program Manager or the PCII Program Manager's designee.

(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 not already authorized to receive such information by the PCII Program Manager or PCII Program Manager's designee, with the exception of their contractors after complying with the requirements of paragraph (c) of this section, or remove any PCII markings, without first obtaining authorization from the PCII Program Manager or the PCII Program Manager's designees, who shall be responsible for requesting and obtaining written consent from the submitter of the information.

(2) State and local governments may use PCII only for the purpose of protecting critical infrastructure or protected systems, or as set forth elsewhere in these rules.

(e) *Disclosure of information to appropriate entities or to the general public.* PCII may be used to prepare advisories, alerts, and warnings to relevant companies, targeted sectors, governmental entities, ISAOs or the general public regarding potential threats and vulnerabilities to critical infrastructure as appropriate pursuant to the CII Act. Unless exigent circumstances require otherwise, any such warnings to the general public will be authorized by the Secretary, Under Secretary for Preparedness, Assistant Secretary for Cyber Security and Telecommunications, or Assistant Secretary for Infrastructure Protection. Such exigent circumstances exist only when approval of the Secretary, the Under Secretary for Preparedness, Assistant Secretary for Cyber Security and Telecommunications, or the Assistant Secretary for Infrastructure Protection cannot be obtained within a reasonable time necessary to issue an effective advisory, alert, or warning. In issuing advisories, alerts and warnings, DHS shall consider the exigency of the situation, the extent of possible harm to the public or to critical infrastructure, and the necessary scope of the advisory or warning; and take appropriate actions to protect from disclosure any information that is proprietary, business sensitive, relates specifically to, or might be used to identify, the submitting person or entity, or any persons or entities on whose behalf the CII was submitted, or is not otherwise appropriately in the public domain. Depending on the exigency of the circumstances, DHS may consult or cooperate with the submitter in making such advisories, alerts or warnings.

(f) *Disclosure for law enforcement purposes and communication with submitters; access by Congress, the Comptroller General, and the Inspector General; and whistleblower protection.*—(1) *Exceptions for disclosure.* (i) PCII shall not, without the written consent of the person or entity submitting such information, be used or

disclosed for purposes other than the purposes of the CII Act, except—

(A) In furtherance of an investigation or the prosecution of a criminal act by the Federal government, or by a State, local, or foreign government, when such disclosure is coordinated by a Federal law enforcement official;

(B) To communicate with a submitting person or an authorized person on behalf of a submitting entity, about a submittal of information by that person or entity when authorized to do so by the PCII Program Manager or the PCII Program Manager's designee; or

(C) When disclosure of the information is made by any officer or employee of the United States—

(*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 Government Accountability 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 DHS through the PCII Program Manager.

(2) Consistent with the authority to disclose information for any of the purposes of the CII Act, disclosure of PCII may be made, without the written consent of the person or entity submitting such information, to the DHS Inspector General.

(g) *Responding to requests made under the Freedom of Information Act or State, local, and tribal information access laws.* PCII shall be treated as exempt from disclosure under the Freedom of Information Act and any State or local law requiring disclosure of records or information. Any Federal, State, local, or tribal government agency with questions regarding the protection of PCII from public disclosure shall contact the PCII Program Manager, who shall in turn consult with the DHS Office of the General Counsel.

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

(i) *Restriction on use of PCII in civil actions.* Pursuant to section 214(a)(1)(C) of the Homeland Security Act of 2002, PCII 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, State, local, or tribal law.

§ 29.9 Investigation and reporting of violation of PCII procedures.

(a) *Reporting of possible violations.* Persons authorized to have access to PCII shall report any suspected violation of security procedures, the loss or misplacement of PCII, and any suspected unauthorized disclosure of PCII immediately to the PCII Program Manager or the PCII Program Manager's designees. Suspected violations may also be reported to the DHS Inspector General. The PCII Program Manager or the PCII Program Manager's designees shall in turn report the incident to the appropriate Security Officer and to the DHS Inspector General.

(b) *Review and investigation of written report.* The PCII Program Manager, or the appropriate Security Officer shall notify the DHS Inspector General of their intent to investigate any alleged violation of procedures, loss of information, and/or unauthorized disclosure, prior to initiating any such investigation. Evidence of wrongdoing resulting from any such investigations by agencies other than the DHS Inspector General shall be reported to the Department of Justice, Criminal Division, through the DHS Office of the General Counsel. The DHS Inspector General also has authority to conduct such investigations, and shall report any evidence of wrongdoing to the Department of Justice, Criminal Division, for consideration of prosecution.

(c) *Notification to originator of PCII.* If the PCII Program Manager or the appropriate Security Officer determines that a loss of information or an unauthorized disclosure has occurred, the PCII Program Manager or the PCII Program Manager's designees shall notify the person or entity that submitted the PCII, unless providing such notification could reasonably be expected to hamper the relevant investigation or adversely affect any other law enforcement, national security, or homeland security interest.

(d) *Criminal and administrative penalties.* (1) 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 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.

(2) In addition to the penalties set forth in paragraph (d)(1) of this section, if the PCII Program Manager determines that an entity or person who has received PCII has violated the provisions of this Part or used PCII for an inappropriate purpose, the PCII Program Manager may disqualify that entity or person from future receipt of any PCII or future receipt of any sensitive homeland security information under section 892 of the Homeland Security Act, provided, however, that any such decision by the PCII Program Manager may be appealed to the Office of the Under Secretary for Preparedness.

Michael Chertoff,

Secretary.

[FR Doc. 06–7378 Filed 8–31–06 8:45 am]

BILLING CODE 4410–10–P