Protected Critical Infrastructure Information Program

Procedures Manual

April 2009

PCII PROGRAM PROCEDURES AND GUIDANCE MANUAL

As you read this Manual and participate in the PCII Program, you may have further questions and concerns regarding the PCII Program procedures. The PCII Program Office welcomes your questions and comments. Please find contact information for the PCII Program Office below. The PCII Program Office can be reached during Federal government business hours to answer any questions regarding the PCII Program.

	PCII PROGRAM OFFICE CONTACT INFORMATION
Telephone	202-360-3023
Facsimile	703-235-3050
E-mail	***pcii-info@dhs.gov***
Web site	www.dhs.gov/pcii

TABLE OF CONTENTS

LIST OF APPENDICES

LIST OF TABLES

NOTE: This version supersedes Volumes I, II, and III of the PCII Program Procedures Manual published in December 2005.

1. INTRODUCTION

This Protected Critical Infrastructure Information (PCII) Program Procedures Manual (Manual) provides guidance governing PCII and the PCII Program as established by Section 214 of the Critical Infrastructure Information Act of 2002 (CII Act)[1] and Section 29.4(b)(4) of the implementing Regulation[2] (Regulation). Terms and acronyms used herein are defined in Appendix 2, Definitions. This revised Manual reflects the evolution of the PCII Program as an information sharing tool, the operational experience the PCII Program Office gained over the last 3 years, and the issuance of the Regulation in September 2006 that amended the interim rule under which the PCII Program had been operating. The Secretary of Homeland Security designated the Under Secretary of the National Protection and Programs Directorate as the senior DHS official responsible for the direction and administration of the PCII Program and the PCII Program Manager (PM), appointed by the Under Secretary, administers the PCII Program's daily operations.

PCII is a category of Sensitive but Unclassified (SBU) information that is afforded protections from (a) disclosure under the Freedom of Information Act (FOIA) and similar State and local disclosure laws and (b) use in civil litigation or for regulatory purposes. The PCII Program is unique because it provides a method for critical infrastructure owners to submit information voluntarily to the Federal government that the government would not otherwise have access to. Once information is submitted and the PCII Program has validated it as PCII, Federal, State, and local government entities can use the information to protect the Nation's critical infrastructure. PCII is accessed only by authorized users who have a need-to-know specified PCII.

The Regulation directed the PM to establish procedures to ensure that any DHS component or other Federal, State, or local entity that works with PCII understands and implements the policy and procedural requirements necessary to appropriately receive, handle, and safeguard PCII in compliance with the requirements of the CII Act and the Regulation. This Manual therefore is designed to allow PCII Program participants to adapt and construct operational procedures in a format that best meets each entity's needs. To that end, the requirements set forth in this Manual describe what an entity's PCII program must accomplish, but in general are not meant to narrowly prescribe how the entity should achieve compliance with a requirement or procedure. This Manual should be supplemented by standard operating procedures (SOPs) tailored to the individual entity.

Contact the PCII Program Office during business hours to answer any questions regarding the PCII Program and this Manual. Additional information, including contact information, is located on the PCII Program Office Web site: **http://www.dhs.gov/pcii.**

---

1 Title II, Subtitle B, of the *Homeland Security Act of 2002*, Public Law 107-296, 116 Statute 2135 (6 U.S.C. 131 *et seq.*).

2 6 Code of Federal Regulations, Part 29, as amended. Also known as *Procedures for Handling Protected Critical Infrastructure Information; Final Rule*.

2. ROLES AND RESPONSIBILITIES

In addition to the PCII PM and the staff of the PCII Program Office within DHS, other participants assist in the implementation of the PCII Program across Federal, State and local governments. This section describes the roles of the PCII Officer, Deputy Officer and the PCII Program Manager's Designee who are responsible for implementing the PCII Program within their respective entities.

2.1 PCII OFFICER RESPONSIBILITIES

Each Federal, State, and local government entity electing to participate in the PCII Program must have a PCII Officer who is responsible for ensuring that PCII received by that entity is used, safeguarded, stored, and disseminated in accordance with the requirements set forth in the CII Act, the Regulation, and all other guidance promulgated by the PCII PM. Every PCII user will be assigned to a PCII Officer who is responsible for ensuring that the individual has met all the access requirements. Users should contact the PCII Program Office if they do not know who their PCII Officer is.

Table 2-1 sets forth the various roles and responsibilities of a PCII Officer. Depending on the breadth and structure of a PCII program within a given government entity, the PCII Officer may also serve as the PCII PM's Designee (described in Section 2.2, "PCII Program Manager's Designee") and/or the senior official executing with DHS the Memorandum of Agreement (MOA) (described in Section 10.4, "Memorandum of Agreement"). If the PCII Officer and Designee are different individuals, the PCII Officer will oversee the Designee for all PCII-related activities and ensure that the Designee properly assumes his or her roles and responsibilities. The PCII Officer should have a Deputy PCII Officer to assist in the execution of his or her duties. The PCII Officer can also nominate Assistant PCII Officers to assist in the practical management of the PCII Program within his or her entity.

Table 2-1. PCII Officer's and Deputy PCII Officer's Roles and Responsibilities

	PCII Officer's and Deputy PCII Officer's Roles and Responsibilities
1	Demonstrate full familiarity with the minimum requirements for protecting information according to the CII Act, the Regulation, and the procedures established by the PCII PM.
2	Implement requirements set forth in the MOA. A draft of the MOA can be found in Appendix 14 (Federal) and Appendix 15 (State/local).
3	Certify, as appropriate, or assist the PCII PM in certifying, contractors requiring access to PCII, including confirming that their contracts contain appropriate language requiring compliance with PCII Program Office guidance.
4	Ensure the secure sharing of PCII with appropriate authorities and individuals, including: Responding to or assisting with need-to-know inquiries Assisting the PCII Program Office in delivering initial and ongoing training Assisting the PCII Program Office in having the nondisclosure agreements executed and implemented.
5	Designate Assistant PCII Officers as necessary to assist in program implementation.
6	Implement operational procedures, pursuant to guidance given by the PCII Program Office, to ensure that PCII and work products, including derivative materials, alerts, warnings, and advisories, are used, handled, and disseminated appropriately and safeguarded properly. Appendix 8, Guide for PCII Work Products, provides more information.

	PCII Officer's and Deputy PCII Officer's Roles and Responsibilities
7	Establish and maintain an ongoing self-inspection program, including periodic review and assessment of the handling, use, and storage of PCII.
8	Coordinate the preliminary investigation into any suspected or actual misuse or loss of PCII. Immediately report any suspected or actual misuse, loss, or unauthorized dissemination of PCII or any suspicious or inappropriate request for PCII to the PCII PM.
9	Ensure that their respective Disclosure Officers are aware that PCII is a Federal record so that the Disclosure Officers are prepared to make an appropriate response to requests for PCII under their respective disclosure laws. The State or local Disclosure Officers must inform requesters that PCII is a Federal record, and that the CII Act protects it from disclosure under all disclosure laws. If the requester has any further questions about the applicability of disclosure laws to PCII, State and local participating entities are encouraged to refer the requester directly to the PCII Program Office or the National Protection and Programs Directorate Disclosure Office.
10	Ensure that the entity's oversight and compliance activities follow PCII Program Office guidance. Develop and implement a process by which the Designee (if applicable) and the entity's PCII Officer will be immediately informed of any suspected violation of PCII security procedures, the loss or misplacement of PCII, or any suspected unauthorized disclosure of PCII within the Designee's entity or entities.
11	Coordinate promptly and appropriately with the PCII PM regarding any request, challenge, or complaint arising from the implementation of the Regulation at 6 C.F.R. Part 29.
12	Participate in meetings with the PCII Program Office, PCII Officer working groups, and other coordination activities regarding PCII, as appropriate.
13	Initiate, facilitate, and promote activities to foster and maintain awareness of PCII policies and procedures.
14	If approached by a potential submitter, act as a PCII advocate to the private sector by providing guidance on appropriate points of contact and courses of action.
15	Participate regularly in PCII training sessions to maintain awareness of program developments.
16	To the extent practicable, remind individuals of their post-employment or PCII program responsibilities.

2.2 PCII PROGRAM MANAGER'S DESIGNEE

The PCII PM will appoint a Designee when critical infrastructure information (CII) will be submitted for PCII protection to a Federal entity other than the PCII Program Office (see Section 3.8, "Submission of Information under a Categorical Inclusion"). The Designee is a Federal employee appointed by the PCII PM to assist in the implementation of the CII Act and the Regulation within the Designee's entity. The PCII PM appoints the Designee when the PCII Program Office and a Federal government entity establish a categorical inclusion (see Section 3.8, "Categorical Inclusion"). On a case-by-case basis, the PCII PM will delegate to this individual certain managerial and administrative responsibilities and functions of the PCII Program Office as set forth in Table 2-2. The Designee would generally be appointed when critical infrastructure information will be submitted to an entity other than the PCII Program Office. A PCII Officer, whose roles and responsibilities are discussed in Section 2.1, "PCII Officer Responsibilities", may also serve as the Designee.

Within the context of PCII accepted as part of a categorical inclusion, the Designee acts as an extension of the PCII Program Office. The Designee will have an active role in the receipt and marking of CII qualifying under a specified categorical inclusion. If an entity's PCII Officer and PCII PM's Designee are two different people, the PCII Officer will oversee the Designee who is responsible for issues related to the entity's PCII program. Depending on mission requirements, there may be multiple Designees within a Federal entity. In addition, a single Designee can be responsible for multiple categorical inclusions within a Federal entity.

The PCII PM will generally appoint a Designee during or after an entity's accreditation process (see Section 10, "Accreditation") has been completed and only when the particular government entity slated to receive CII has—

- Appointed a PCII Officer (who can also be the Designee provided the PCII Officer is a Federal government employee)
- Requested that the CII be submitted as part of a categorical inclusion
- Trained the necessary staff in PCII procedures
- Implemented measures to comply with the Regulation
- Agreed that the PCII Program Office may at any time verify that entity's compliance with the Regulation and other Program requirements.

The Designee will undertake training as required by the PCII Program Office (see Table 2-2).

Table 2-2. Designee Roles and Responsibilities

	Designee's Roles and Responsibilities Relating to Categorically Included PCII
	Receiving CII
1	Ensure that all CII submitted under a categorical inclusion includes an express statement affirming that the information is being voluntarily submitted in expectation of the protections provided by the CII Act. If a submission made under a categorical inclusion does not include the express statement, inform the submitter within 30 calendar days of receipt that the submission was procedurally defective and either return or destroy the information.
2	In the case of an e-mailed submission, ensure that the following three statements are received within a reasonable period after the submission: • An electronically-submitted express statement • A non-electronically submitted express statement • A document that memorializes the nature of the initial electronic submission.
3	If the information submitted as CII is accompanied by an express statement, contact the submitter within 30 calendar days of receipt by delivery means prescribed in procedures developed by the PCII PM to acknowledge receiving the information.
4	Within 30 calendar days of receipt, provide the submitting person or entity with a unique Identification Number for the submitted information.
5	Provide to the PCII Program Office the appropriate metadata for all submissions made under a categorical inclusion, so that this metadata may be entered into the PCII Management System.
6	Provide the PCII Program Office access to all information submitted for protection under the CII Act. The access terms are defined in the Agreement to Operate.
7	Ensure that all submissions are accompanied by a certification statement, which is signed by the submitting person or an authorized person on behalf of an entity and identifies the submitting person or entity. The certification statement must contain such contact information as is considered necessary by the PCII PM and certify that the information being submitted is not customarily in the public domain.
	Marking PCII
8	Mark as PCII any information qualifying for PCII protection under a categorical inclusion.
9	Obtain authorization from the PCII Program Office before removing any PCII markings.
	Disseminating and Safeguarding PCII
10	Ensure that the protocols for the dissemination of original PCII adhere to the CII Act and the Regulation and that the information is used only for appropriate purposes.
11	Develop, implement, and maintain processes and procedures to ensure that all PCII is safeguarded appropriately and in a manner consistent with guidance from the PCII Program Office, the DHS Office of Security, or any other appropriate DHS guidance.

	Designee's Roles and Responsibilities Relating to Categorically Included PCII
12	Take immediate action to respond to events—or remedy systemic conditions—that jeopardize the adequate protection of original PCII.
	Management of PCII Program
13	Implement or oversee the implementation of the requirements set forth in the Agreement to Operate and the System Requirements Document.
14	Participate in meetings with the PCII Program Office and in other coordination activities regarding PCII, as appropriate.
15	Cooperate with the PCII Program Office and the PCII Officer in verifying the Designee's compliance with the responsibilities set forth herein and the requirements promulgated by the PCII Program Office.
	Training
16	Complete any training courses required by the PCII Program Office. Participate regularly in PCII training sessions to maintain awareness of program developments.
17	Demonstrate familiarity with the minimum requirements for protecting information according to the CII Act, the Regulation, and the procedures established by the PCII PM.
	Communications with Submitters
18	Authorize—when appropriate and only in the performance of services in support of the purposes of the CII Act—a Federal, State, or local contractor to communicate with a submitting person or an authorized person of a submitting entity about a submission of categorically included information by that person or entity.
	Investigating and Reporting Violation of PCII Procedures
19	Report any suspected violation of PCII security procedures, the loss or misplacement of PCII, or any suspected unauthorized disclosure of PCII concurrently to the PCII PM and the PCII Officer.

3. SUBMISSION REQUIREMENTS

This section provides submitters with instructions for submitting CII to DHS in consideration of the protections provided by the CII Act. The guidance set forth in this section implements Section 29.5 of the Regulation, "Requirements for Protection", and describes—

- Submissions
- The submitter community
- The documentation that must accompany submissions before they can be validated
- The means by which the recipient of a CII submission can, prior to validation, request additional information about a submission
- Submission format
- Post-submission responsibilities
- Removal of PCII protections and withdrawal of submissions
- The submitter's latitude in defining the eligible recipients of submitted CII.

3.1 SUBMISSION PROCESS TO DHS AND DESIGNEE

The CII Act requires that all submissions of CII for which CII Act protection is requested be voluntarily submitted to DHS, directly or indirectly. *Submission to DHS*, as referenced in these procedures, means any transmittal of CII to the DHS PCII PM or to any one of the Designees, with a request for protection under the CII Act. Designees will primarily receive CII submissions that fall under the categorical inclusion for which that Designee is responsible (see Section 3.8, "Categorical Inclusion").

Only the PCII Program Office is authorized to validate a submission as PCII. When the information is part of a categorical inclusion, the PCII PM will have previously declared certain subject matter or types of information categorically protected as PCII, and the information will be considered validated as PCII upon receipt by the PCII Program Office or the Designee. If anyone other than the PCII PM or Designee receives CII for validation as PCII, he or she should return it to the submitter or give it to the PCII PM for validation.

A submitter may want to identify particular Federal, State, or local government entities that should receive the information after its validation as PCII. These specifications ensure that the intended government entity can access the particular PCII expeditiously. The submitter should work with the PCII Program Office or the Designee, as applicable, to designate recipients of a given PCII submission.

3.1.1 Submitter Community

Sources anticipated to submit CII for consideration for protection are those with knowledge about the security of a critical infrastructure and include but are not limited to—

- Information sharing and analysis organizations (ISAOs)
- State and local government officials
- Representatives of privately or publicly owned companies
- Industry associations (on behalf of their members)
- Individuals capable of providing an analytical observation of a critical infrastructure..

Any party submitting CII to the PCII Program in consideration of the protections of the CII Act must—

- Own the information (or be an authorized representative of the owner of the information), and
- Have sufficient knowledge of the information to complete an Express Statement (see Section 3.2, "Express Statement") and a Certification Statement (see Section 3.3, "Certification Statement").

Federal entities may not submit information for protection under the CII Act.

3.1.2 Submitting Information for PCII Validation

The steps below outline the procedures a submitter must follow when submitting CII for validation as PCII—

1. The submitter decides that PCII protection for his or her CII is a necessary precondition for sharing the information with a Federal, State, or local government entity.
2. The submitter determines whether to submit his or her CII to the PCII Program Office or a Federal entity designated to receive CII under a categorical inclusion.
3. The submitter includes an Express and signed Certification Statement (See Appendix 5) with the submission.
4. If the submitter wishes to limit dissemination to specific government agencies, a statement requesting limited dissemination must accompany the submission (see Section 8.2.1, "Requested Limited Dissemination PCII").
5. The submitter submits his or her CII to the PCII Program Office or a Designee. Directions for submission are set forth in Section 3.4, "Format of Submission". Submission to a Designee will require coordination with that Designee to define the method of submission. *(Note: Should a submission be made to a Designee, that Designee is responsible for forwarding the submission-related metadata to the PCII Program Office.)*

3.2 EXPRESS STATEMENT

All submissions must include a statement affirming the information is being submitted in expectation of PCII protections and in the absence of an exercise of legal authority by DHS to compel access to or submission of the information. This statement is known as the "Express Statement." Any submission to the PCII Program that includes an Express Statement will be granted the presumption of PCII protection from the moment it is received by the Program. Submissions without an Express Statement will be destroyed and a follow-up request for a new submission will be made. (This is necessary because submissions made without an Express Statement do not have the presumption of protection). The Express Statement must be a written statement 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."

The Express Statement form is provided in Appendix 5.

3.3 CERTIFICATION STATEMENT

All submissions made in consideration of the protections of the CII Act must include a Certification Statement certifying that the information is—

- Not being submitted in lieu of independent compliance with a Federal legal requirement
- Of a type not customarily in the public domain.

In the Certification Statement, the submitter must affirm that the individual submitting the information for protection under the CII Act is authorized to submit the information.

The Certification Statement also informs the submitter that any knowing or willful false representations on such submissions may constitute a violation of 18 U.S.C. §1001 and are punishable by fine and imprisonment.

The submitter must also provide contact information. This information becomes important if additional information is required for validating the CII, an authorized user of the submitted CII has questions about the information, or if the consent of the submitter is required to disclose the submitted CII.

CII submitted with the Express Statement but without a complete Certification Statement will have the presumption of PCII protection and may enter the validation process. The validation process cannot be completed, however, until the PCII Program Office receives a complete Certification Statement. Should the PCII Program receive a CII submission with an incomplete or improper Certification Statement, within 30 calendar days of receiving the submission, it will inform the submitter that the submission was procedurally defective. The submitter will have 30 calendar days in which to provide the required Certification Statement. If a Certification Statement has not been received for the submission in question after 30 calendar days, the PCII Program Office or Designee will inform the submitter that the submitted information does not qualify for PCII protection and will follow the procedures in Section 5, "Validation", for rejecting a submission.

The Certification Statement form is provided in Appendix 5.

3.4 FORMAT OF SUBMISSIONS

The CII Act does not specify the format in which information must be submitted. When determining the format of a submission, the submitter should consider how the authorized PCII user will ultimately use the information. When responding to a request from a government entity, the submitter should coordinate with the requesting entity to identify the best format for submitting the information. In the case of an unsolicited submission, the submitter should choose common formats and select electronic over paper whenever possible.

All submissions should provide certain information that helps categorize the submission and helps the PCII Program Office manage the broad array of submitted information. The following information should be provided with all submissions:

- If the information was created as part of an ISAO, a list of the participants in the ISAO
- A statement of the Critical Infrastructure/Key Resource Sector that applies to the submission
- A brief description or abstract of the submission
- The physical location of the Critical Infrastructure/Key Resource
- Any applicable directions for sharing the submitted information with specific government agencies or individuals.

The following sections provide details on several submission methods accepted by the PCII Program Office.

3.4.1 Submission of Physical Materials

Physical materials include paper copies and digital media, such as floppy discs, compact discs, video tapes, and audio tapes. The PCII Program Office or its Designees accept submissions in various physical formats (e.g., a submitter may put an electronic file on a compact disc and send it to the Program Office or Designee through the mail). If a submitter wishes to mail a submission to the PCII Program Office, the address is:

Department of Homeland Security
PCII Program Office
245 Murray Lane, SW
Bldg 410
Washington, D.C. 20528-0001

3.4.2 Electronic Submissions

Submitters may use any mode of electronic transmission they consider appropriate for the sensitivity of the data being submitted, provided that the PCII Program Office has the technical and operational capabilities required for receiving such transmissions. The PCII Program Office accepts submissions via fax and e-mail and through its Web site, as set forth in Table 3-1 below. The submitter must contact the PCII Program Office before submitting any data feeds to ensure that the PCII Program Office is prepared to receive the submission. If the submission is intended for a particular recipient, the PCII Program Office must also determine whether that recipient is capable of receiving the transmission in the submitter's format.

Table 3-1. Submission Methods

Submission		
Fax	E-mail	Web
703-235-3050	***pcii-submit@dhs.gov***	***http://www.dhs.gov/pcii***

3.4.3 Oral Submissions

Information may be submitted orally to the PCII Program provided that a written statement memorializing the oral information is submitted within 15 calendar days following the oral communication. The initial oral submission must be accompanied by an oral request to have the information protected under the provisions of the CII Act. If a Designee receives an oral submission that is not related to a categorical inclusion, the Designee should forward it to the PCII Program Office.

The PCII Program Office or Designee will record all oral submissions to ensure accuracy. This means that face-to-face oral submissions will not be accepted unless the submitter has made prior arrangements with the PCII Program Office or Designee to record the submission. The PCII Program Office or Designee will work with submitters to ensure that, when circumstances require, oral submissions are validated and recorded in a timely manner. Oral submissions will have the presumption of PCII protection from the time the submitter verbally requests that the information be protected as PCII until the time the PCII PM makes a final validation determination.

The PCII Program Office (or Designee) must receive a document memorializing the nature of the oral submission within 15 calendar days of its submission. This written statement must include an Express Statement and a complete Certification Statement. If the PCII Program Office or Designee does not receive the required written statement described above within 15 calendar days after the oral submission is made, the recording of the oral submission will be destroyed in accordance with the PCII Program Office records schedule.

Oral submissions will not be entered into the PCII Management System (PCIIMS) or validated until the written statement is received by the PCII Program Office. Upon receipt of the written statement, validation of the oral submission will be the same as for any other submission. Once an oral submission is validated as PCII, the original record of that submission will be destroyed.

3.4.4 Other Considerations

In some cases the PCII Program Office may not have the technological and operational capability to receive, process, and share information in a particular format. For the most current information regarding the PCII Program's capability to accept submissions in various formats, contact the PCII Program Office via e-mail [pcii-info@dhs.gov] or check the PCII Program Web site [www.dhs.gov/pcii]. If submitting CII to a Designee, coordinate with that Designee to determine which methods of submission are acceptable.

3.5 SAFEGUARDING ELECTRONICALLY SUBMITTED INFORMATION

The PCII Program strongly encourages submitters to encrypt their CII when submitting it electronically to the PCII Program Office or Designee. The PCII Program Office's standard encryption is PGP® and the PCII Program Office's public key is available to anyone who wishes to submit CII. The PCII Program Office may be able to accommodate other encryption methods. Before transmitting submissions using any encryption method other than PGP, a submitter must contact the PCII Program Office to confirm that it has the capability to receive the submission in

the desired encryption method. If it does not have that capability, the PCII Program Office will work with the submitter to find an acceptable alternative.

Submitters may choose other methods to protect information submitted electronically. These may include password-protecting the files or using a compression technology that provides information encryption.

3.6 REQUESTS FOR ADDITIONAL INFORMATION AFTER RECEIPT

The PCII PM or Designee may contact the submitter if the following material is not provided in a submission:

- An Express Statement (in the case of a missing Express Statement, the original submission will be destroyed and a request will be made for resubmission)
- Certification Statement.

The PCII PM or Designee may also contact the submitter if the submitted CII appears incomplete or is damaged in some way that prevents a validation determination. Additional correspondence may occur during the validation process and is detailed in Section 5, "Validation".

The PCII PM or Designee may request more information from the submitter. The submitter must respond within 30 calendar days of the request, even if the response is a request for additional time in which to provide the requested information. If the submitter does not respond within 30 calendar days, the submission will be destroyed.

3.7 POST-SUBMISSION RESPONSIBILITIES

Following the submission of information for protection, submitters remain responsible for responding to requests from the PCII Program Office regarding that information. These requests may relate to the validation process or, under certain conditions, the handling, use or dissemination of the information. Submitters are generally requested to respond within 30 calendar days from the receipt of a request. In most cases, if no response is received, the PCII Program Office can take no further action. For example, a submitter may be asked to complete any of the following tasks after the initial submission:

- Resubmit, if an Express Statement was not provided.
- Provide a Certification Statement.
- Fully complete contact information if all such information was not included in the original submission.
- Replace any information that may be corrupted, damaged, or unreadable.
- Provide additional information to confirm the submission is eligible for validation as PCII.
- Consider providing updated information regarding the submission, as well as any updates to the submitter's contact information. Such updates include but are not limited to changes in the primary and alternate contacts, the nature or description of provided CII, the ownership of the infrastructure, or any other details since the time of submission.

In some cases, a Designee or authorized user may need to contact a submitter for further clarification about a particular submission. Before doing so, the user should first coordinate with either the Designee or the PCII Officer.

When practicable, the Designee or PCII Officer should ensure that there is a coordinated approach to contacting the submitter to avoid multiple contacts about the same issue.

3.8 SUBMISSION OF INFORMATION UNDER A CATEGORICAL INCLUSION

The PCII PM has discretion to declare certain subject matter or types of information categorically protected as PCII and to set procedures for the receipt and processing of such information. Critical infrastructure information within a categorical inclusion will be considered validated upon receipt by the PCII Program Office or the appropriate Designee without further review if the submitter provides the Express and Certification Statements and the PCII Program Office has pre-validated the information as PCII. Such pre-validated categories of information are referred to as a categorical inclusion.

A Designee must be appointed and trained before an entity can receive submissions under a categorical inclusion. Moreover, only Federal entities can submit requests to the PCII Program Office to receive submissions under a categorical inclusion. Interested parties should coordinate with the PCII Program Office to generate any documentation needed to establish the categorical inclusion.

The steps set forth in Section 3.8.1, "Establishing and Implementing a Categorical Inclusion", outline the procedures a Federal entity must follow in establishing a categorical inclusion. Federal agencies may only receive PCII submissions directly if the information falls within the categorical inclusion for which that entity has responsibility. Categorical inclusions should conform to the following criteria and the PCII Program Office will work with the Federal entity to accommodate its information collection needs:

- The information being submitted is not customarily in the public domain.
- The information being submitted is part of an information sharing partnership.
- Any request for CII from the private sector must be pre-validated by the PCII PM and be designed to elicit a response that meets the definition of CII.
- Any additional queries must be designed to elicit a response that contributes to the understanding of the submitted CII.
- An auditing process is in place that ensures that submissions meet the criteria defined above.

3.8.1 Establishing and Implementing a Categorical Inclusion

The steps below outline the procedures a Federal entity should follow in establishing and implementing a categorical inclusion.

1. A Federal government entity identifies a need to receive CII held outside the Federal Government to fulfill homeland security duties and identifies potential submitters.
2. The Federal government entity submits a request to the PCII PM to allow the direct submission of CII to that entity. The request should include:

- A statement that the intended responses to the proposed request for information would meet the definition of CII;
- An explanation as to why the information is not customarily in the public domain;
- A statement that the request is part of an information sharing partnership; and
- If available, the template or form containing the questions that will generate responses requiring PCII protection or a description of the type of information that will be submitted.

3. The Federal government entity nominates an official to be appointed by the PCII PM as a Designee. This individual must be able to fulfill the roles and responsibilities set forth in Section 2.2, "PCII Program Manager's Designee", and will be required to complete training as directed by the PCII Program Office.
4. The Federal government entity must execute an MOA (see Section 10.4, "Memorandum of Agreement").
5. If a Federal entity is not yet accredited, the entity nominates a PCII Officer. The nominee must be able to fulfill the roles and responsibilities set forth in Section 2.1, "PCII Officer Responsibilities". The PCII Officer and Designee may be the same person.
6. The PCII PM reviews the request, confirms that the type of information likely to be submitted meets the requirements for protection, establishes a categorical inclusion for such information, and informs the requesting Federal government entity that a categorical inclusion has been established.
7. Once the Designee candidate has completed all training prescribed by the PCII Program Office, the PCII PM appoints him or her as a Designee.
8. A senior official with the ability to bind the requesting Federal government entity to an agreement executes an Agreement to Operate (ATO) (see Section 4.3, "Agreement to Operate").
9. The requesting Federal government entity implements the requirements stated in the ATO including, any electronic system requirements for the secure receipt and storage of PCII, if necessary.
10. The requesting Federal government entity solicits information from the submitter community.
11. A submitter willing to submit CII to the Federal government entity states a desire for the information to be protected under the CII Act.
12. The Designee receives CII and ensures the following:

    - An Identification Number is assigned to each submission
    - A Cover Sheet is attached to each submission
    - PCII markings are applied to each submission
    - All properly-submitted CII is safeguarded as PCII
    - The metadata associated with each submission is forwarded to the PCII Program Office
    - PCII is properly disseminated only to authorized PCII users.

- The following information is recorded with respect to the PCII that has been disseminated:
  - The date the PCII was disseminated
  - The Identification Number
  - The recipient's name
  - The recipient's organization
  - The recipient's contact information
  - Any additional information the Designee may think is appropriate.

The Designee must cooperate with oversight activities that the PCII Program Office conducts.

3.8.2 General System Requirements for a Categorical Inclusion

Any categorical inclusion that will require a government entity to receive, store, and disseminate PCII must be developed in coordination with the PCII Program Office, in order to customize the system requirements for application to a specific information management system. The PCII Program Office will test the information management system to determine conformance with these requirements.

In addition to the entity-specific system requirements developed by the PCII Program Office and enumerated in an ATO and a System Requirements Document (SRD), the following list contains several broad requirements of all systems receiving, storing, and/or safeguarding PCII within a categorical inclusion:

- Any system storing PCII shall be configured so that only PCII authorized users with the proper need-to-know have access to PCII.
- The system shall be accessed via Secure Socket Layer (SSL).
- The system shall constantly display the following warning banner on the top of the work space (even if the viewer scrolls within a page) when PCII is being viewed:

**********WARNING**********
PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

DISTRIBUTION: By the authority of the PCII Program Manager, PCII may only be shared with PCII Authorized Users who are currently performing homeland security duties and have a need-to-know. All recipients must handle and safeguard this information according to the Critical Infrastructure Information Act of 2002 (6 U.S.C. §§ 131 *et seq.*) and the Procedures for Handling Critical Infrastructure Information; Final Rule (6 C.F.R. Part 29).

- The system must implement backups of PCII data using a schedule/scheme approved by the PCII Program Office.
- The backup schedule/scheme must have the capability to restore the system to the last known good state.
- All tape backups containing PCII must be marked with the following warning and stored in a secure location, as described in Section 7.2, "Procedures for Safeguarding PCII":

WARNING: PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

- The system must audit all user access to PCII data. Audit data must include but are not limited to:
  - User name
  - User role
  - Date and time of access
  - Data accessed.

- The system must have up-to-date anti-virus software installed.
- If the system allows the user to export or print any file containing PCII, the resulting print-out must follow all PCII marking requirements.
  - The system must print a PCII Program Office-approved Cover Sheet (see Section 6.4, "PCII Cover Sheet"), to be affixed to the front of the printout. The PCII Cover Sheet shall display the PCII Identification Numbers for all PCII contained in the document.
  - All printouts containing PCII must be marked at the top and bottom of each page (or in the header and footer) with the following:

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

3.9 ANONYMOUS SUBMISSIONS

Anonymous submissions cannot receive protection under the CII Act. The Regulation requires submitters to provide a signature and contact information with their submissions; therefore, submissions without signatures and contact information do not meet the requirements for protection.

3.10 REMOVAL OF PCII PROTECTIONS

Submitters may request the withdrawal of CII submissions or a change in the status of a submission from PCII to unprotected CII. To change the status from PCII to unprotected CII, the request must be in writing (a sample change-in-status letter can be found in Appendix 7). For information submitted as part of a categorical inclusion, the PCII Program Office may delegate the authority to change the status of PCII to non-PCII to the Designee in the ATO.

The PCII PM or the Designee will follow the submitter's directions under the following circumstances:

- **Withdrawal of Submissions:** If a submitter wishes to withdraw the submission, and that information has not completed the validation process, the PCII Program Office will return all such information to the submitter or destroy the information, depending on the written request of the submitter.

- **Change of Status:** If the submitter requests in writing that the PCII protections be removed on a submission that has already been validated, the PCII Program Office will do so. In this case, the PCII Program Office may destroy the information or return it to the submitter, depending on the submitter's instructions and availability. Recipients of that PCII will be notified of the final change in status.

4. RECEIPT AND ACKNOWLEDGEMENT

This section documents the procedures used by the PCII Program Office and Designee to receive submissions, acknowledge receipt to the submitter, and track the progress of a submission through the validation process. Under the provisions of the CII Act, only the PCII PM or Designee can officially acknowledge receipt of CII and only the PCII PM can validate CII as PCII. The Designee, however, is empowered to determine whether CII submitted under a categorical inclusion meets the standards set by the PCII PM in his or her approval of the categorical inclusion (see also Section 3.8, "Categorical Inclusion").

4.1 METHOD AND ACKNOWLEDGEMENT OF RECEIPT/TRACKING

The PCII Program Office or Designee must contact the submitter and acknowledge receipt of submitted information within 30 calendar days of its receipt. Acknowledgment of receipt is not a determination of validation, but only a notification to the submitter that the PCII Program Office or the Designee has received the information accompanied by an Express Statement. Upon receipt of information accompanied by an Express Statement, the PCII Program Office or Designee will assign the submission an Identification Number, which will be included on all correspondence regarding that information. See also Section 6, "Marking".

If a validation determination can be made within 2 calendar days of receipt, the PCII Program Office or Designee may combine this acknowledgement of receipt with a validation letter (see Section 5.7, "Determining that a Submission Qualifies for Protection"). For example, if the submission is validated as PCII within 2 calendar days of receipt, the PCII Program Office or Designee will send the submitter a single correspondence that acknowledges receipt of the submission and notifies the submitter that the information has been validated.

In the case of oral submissions, receipt will be acknowledged in writing within 30 calendar days after the PCII Program Office or the Designee receives written Express and Certification Statements and documents memorializing the oral submission. When such a submission is made to the PCII Program Office, an Identification Number is applied when the details of that submission are entered into the PCIIMS. When an oral submission made to a Designee is covered by a categorical inclusion, the submission will be catalogued and marked according to the terms of the categorical inclusion. Any oral submission made to a Designee *not* falling under a categorical inclusion must be directed to the PCII Program Office.

4.2 SYSTEM REQUIREMENTS DOCUMENT

The SRD is a document prescribing detailed instructions and specific requirements that must be implemented in order for an entity to participate in a system-to-system transfer of PCII and receive electronic information under most categorical inclusions. Because of the sensitive nature of PCII, any system designed and built to receive, validate, track, and/or disseminate PCII must satisfy PCII system requirements. The PCII Program Office will work with all government entities that will be party to a system-to-system transfer of PCII or participating in a categorical inclusion to develop a tailored SRD for the nature of that entity's participation.

When there will be a system-to-system transfer of PCII, the government entity should contact the PCII Program Office to discuss the need to fulfill the requirements set forth in an SRD. If an

entity is participating in a categorical inclusion, it must implement an ATO as well as an SRD. The ATO described in Section 4.3, "Agreement to Operate", will bind the government entity that is participating in a categorical inclusion to fulfilling the requirements set forth in the SRD.

4.3 AGREEMENT TO OPERATE

For all categorical inclusions, the government entity overseeing the receipt of included information and the PCII Program Office will enter into an ATO defining the conditions under which that entity will receive categorically included PCII. The ATO will set forth the obligations of the PCII Program Office and the recipient entity with respect to the submitted CII and the validated PCII in the entity's possession. A senior official within the government entity who has the authority to bind that entity to such agreements will execute the ATO.

If, as part of a categorical inclusion, an entity will establish a system to receive electronic CII submissions or transfers of PCII from other systems, that entity must implement the requirements in an SRD. In such cases, the execution of the ATO will bind the entity to fulfilling the requirements set forth in the SRD. (See also Section 4.2, "System Requirements Document").

4.4 RECEIVING INFORMATION UNDER A CATEGORICAL INCLUSION

CII determined to be covered by a categorical inclusion will be considered validated upon receipt by the PCII Program Office or any of the Designees without further review, provided that the submitter provides the Express Statement and the PCII Program Office has pre-validated the information as PCII. (See also Section 3.8, "Categorical Inclusion").

If a Designee receives a CII submission that is not covered by a categorical inclusion, the Designee should forward the entire submission to the PCII Program Office. The Designee should *not* retain a copy of the submission. The Designee should instead retain only the submitter's name and contact information, to be used only for the purposes of informing the submitter of any difficulties in forwarding his or her CII submission to the PCII Program Office.

5. VALIDATION

This section describes the process the PCII Program Office uses to determine whether submissions qualify for validation as PCII. The guidance set forth in this section implements, in part, the direction in the Regulation, Section 29.6, "Acknowledgment of Receipt, Validation and Marking". It also addresses the quality assurance process, which ensures a fair and consistent validation process and specifies the conditions under which a change in PCII status may be made.

Validation is the process for determining whether a CII submission qualifies for PCII protection. The Regulation grants the PCII PM the exclusive authority to validate information as PCII. The PCII PM will, however, designate other DHS employees within the PCII Program Office as Validation Analysts (VAs) by delegating to these employees the authority to review CII submitted for PCII validation. Upon receipt by the PCII Program Office, all CII submissions will be assigned to a VA. Within the PCII Program Office, the operations manager is responsible for ensuring that all submissions are processed promptly upon arrival and that VAs are properly processing submissions.

5.1 DETERMINING SUBMITTER QUALIFICATIONS

The VA assigned to each submission must verify that the submitter is qualified to submit CII to the PCII Program. The PCII Program Office will accept submissions of CII in consideration of the protections of the CII Act from any submitter who:

- Is authorized to submit (i.e., owns the information being submitted, or is an authorized representative of the owner of the information);
- Has sufficient knowledge of the information to affirm that it is being submitted *voluntarily* (i.e., in the absence of an exercise of legal authority by DHS to compel access to or submission of such information); and
- Has sufficient knowledge of the information to affirm in the Certification Statement that the information is *not* customarily in the public domain (i.e., not lawfully, properly, and regularly disclosed generally or broadly to the public).

Sources anticipated to submit CII to the PCII Program include but are not limited to:

- ISAOs
- State and local government officials
- Representatives of privately or publicly owned companies
- Industry associations (on behalf of their members)
- Individuals capable of providing an analytical observation of a critical infrastructure.

Representatives of Federal government entities may *not* submit information to the PCII Program in consideration of the protections of the CII Act.

5.2 MISSING OR INCOMPLETE CERTIFICATION STATEMENT

Provided it is accompanied by an Express Statement, a submission will enjoy the presumption of PCII protection from the moment it is received by the PCII Program Office, but may not be

validated as PCII without a valid Certification Statement (see also Section 3, "Submission Requirements"). The PCII Program Office will review the Certification Statement to determine whether the submitter has attested to all of the applicable requirements of the Regulation.

If the Certification Statement is missing or incomplete at the time of submission, the PCII Program Office will contact the submitter within 30 calendar days of receipt of the submission to request that a proper Certification Statement be completed for the submission in question and sent to the PCII Program Office. The submitter will have 30 calendar days to respond to this request.

If the submitter does not respond to the PCII Program Office's request within 30 calendar days of receipt of the request, the PCII Program Office may determine that the presumption of PCII protection is terminated, notify the submitter that the submission does not qualify as PCII and return the information to the submitter or destroy it, according to the submitter's instructions.

If the submitter complies with the request and provides the PCII Program Office with a proper Certification Statement for the submission, the VA assigned to the submission may proceed to the next step in the validation process (see Section 5.5, "Requesting Additional Information to Make Validation Determination").

5.3 DETERMINING WHETHER A SUBMISSION IS CII

To be validated as PCII, submitted information must meet the definition of CII set forth in Appendix 2, Definitions.

The VA will review submitted information to determine whether it meets the definition of CII. If it is determined that a submission does not meet the definition of CII, it must be returned to the submitter or destroyed, in accordance with Section 5.8, "Disposition of Rejected Submissions".

5.4 DETERMINING WHETHER A SUBMISSION IS CUSTOMARILY IN THE PUBLIC DOMAIN

Upon determining that a submission meets the definition of CII, the VA assigned to the submission will consult various sources to determine whether the submission contains information that is customarily in the public domain. The VA must independently determine that submitted information is not customarily in the public domain and will not rely solely on the submitter's statements or assertions.

The VA may consult the following sources in making this determination:

- The Internet
- Internal or external industry experts or analysts
- Subscription information services, such as Lexis Nexis©
- The Web page of the entity submitting the information
- Publicly available financial reports of the submitting entity
- Televised news
- U.S. Securities and Exchange Commission filings
- Newspaper articles
- Magazine articles

- Information provided for a public administrative procedure, such as a utility rate-making decision
- Trade publications or other industry sources.

If the entire content of a submission is in the public domain, the VA assigned to the submission will reject it as PCII. If only portions of a submission are customarily in the public domain, the submission will not be rejected.

Some information may be available to the public, but not considered to be in the public domain. The VA must decide whether the information is readily available to the public or whether some additional transaction is required to gain access to the information.

5.5 REQUESTING ADDITIONAL INFORMATION TO MAKE VALIDATION DETERMINATION

If the VA assigned to a submission makes an initial determination that it does not qualify for PCII protection, the following procedure will be followed:

1. The VA will notify the submitter of the initial determination that the information does not qualify for PCII protection.
2. The VA will ask the submitter to further explain the submission and the submitter's basis for believing the information qualifies for protection as PCII. Whenever possible, the VA will tell the submitter what type of additional information is needed.
3. The VA will request the submitter to indicate whether the submission should be retained without the protections of the CII Act, returned to the submitter, or destroyed should the PCII Program Office determine that the submitter's information is not PCII.
4. The submitter has 30 calendar days from the date of the correspondence to respond to the request.
5. If additional information is received within 30 calendar days, the VA will review the information and determine whether the submission qualifies for PCII protection. The VA will then follow the procedures set forth in Section 5.7, "Determining That a Submission Qualifies for Protection".
6. If additional information is not received within 30 calendar days, the submission will be rejected as PCII and returned to the submitter or destroyed, depending on the submitter's written preference. If return to the submitter is impractical or if the submitter did not provide instructions for returning the submission, the PCII Program Office will destroy the information within 30 calendar days, consistent with the appropriate National Archives and Records Administration-approved records disposition schedule.

5.6 HANDLING PCII DURING VALIDATION

All submissions of CII to the PCII Program that include an Express Statement will enjoy the presumption of protection from the moment of receipt by the Federal government. These submissions are handled, stored, and safeguarded as PCII. (See Section 7, "Safeguarding").

Submissions made in consideration of PCII protection should only be reviewed in designated PCII processing areas and in a manner that precludes access by individuals not authorized to view PCII and those without a valid need-to-know for the submission. Being assigned to validate a CII submission constitutes a valid need-to-know for a VA.

If the VA contacts the submitter for more information about a particular submission, the contact must be documented and safeguarded in accordance with PCII requirements. Any letters sent to the submitter must be treated as PCII, because they contain identifying information about the submitter.

5.7 DETERMINING THAT A SUBMISSION QUALIFIES FOR PROTECTION

If an appropriate Express Statement and a complete Certification Statement (see Section 3, "Submission Requirements") accompany a submission, the PCII Program Office will review the submission to determine whether it meets the definition of CII and is voluntarily submitted.

If the VA(s) determines that the information is PCII, the submission is sent to the PCII PM for approval. If the PCII PM agrees with the validation determination, he or she will sign a Validation Letter, which will be sent to the submitter to inform him or her of the validation determination. If the submission is made through the e-submissions Web portal, the VA will send an e-mail informing the submitter of the disposition of his or her submission. If the PCII PM determines that the information is not PCII, he or she will sign a Rejection Letter, informing the submitter that the submitted CII was not validated as PCII. The PCII Program Office will then follow the procedures set forth in Section 5.8, "Disposition of Rejected Submissions".

5.7.1 Validated as PCII

When a submission is validated as PCII, the submitter will be informed by means of a Validation Letter.

When a submission is validated as PCII, the assigned VA will enter the submission metadata into the PCIIMS. The VA will ensure that the information is properly marked according to the parameters defined in Section 6, "Marking", and that the submission is stored according to the procedures defined in Section 7, "Safeguarding".

5.7.2 Rejected as PCII

If it is determined that a submission should *not* be validated as PCII, a Rejection Letter will be sent to inform the submitter of the determination.

5.8 DISPOSITION OF REJECTED SUBMISSIONS

When it is determined that a submission is not PCII, the PCII Program Office will, within 30 calendar days of the final determination, destroy the submission or return it to the submitter in accordance with the submitter's written preference (obtained in the procedures described in Section 5.5, "Requesting Additional Information to Make Validation Determination"). If return to the submitter is impractical, the PCII Program Office will destroy the information within 30 calendar days. If the submission was made to a Designee or indirectly through another Federal

government entity, the PCII Program Office will direct the initial recipient to retain the Identification Number and destroy all copies of the submission (and any identifying information about the submission).

A submission should be returned to the submitter in the same manner in which it was received, unless the submission was made orally or sent by e-mail. In the case of an oral submission, the documentation supporting the submission must be destroyed or returned to the submitter by mail, based on the submitter's preference. Rejected e-mail submissions must be destroyed.

When a submission is to be destroyed, the destruction must be consistent with the appropriate National Archives and Records Administration-approved records disposition schedule. See Section 11, "Destruction of PCII".

5.9 RECORDING INFORMATION IN THE PCIIMS

The PCII Program Office has developed an electronic management system known as the PCIIMS. The PCIIMS serves to record the receipt, acknowledgement, validation, storage, dissemination, and destruction of PCII, including PCII in repositories that store original PCII.

The PCII Program Office has defined a specific set of metadata that describes the submitter, the CII involved, and the status of the submission. The metadata for all submissions will be entered into the PCIIMS, including the metadata that the Designee must send to the PCII Program Office that is associated with any PCII the Designee receives as part of a categorical inclusion. For all repositories of original PCII, the PCIIMS records—

- Receipt of submissions
- Contact information of the submitter and Designee
- Validation determinations
- Storage location of original PCII
- Amendments or additions to original PCII submissions

The PCIIMS is able to generate the PCII card catalog, which contains a brief description and the location of all original PCII. The card catalog does not contain actual PCII. To facilitate information sharing, this catalog is accessible to all authorized users of PCII.

5.10 POST-VALIDATION CHANGE IN STATUS

In some cases, the PCII PM may discover that information validated as PCII did not, in fact, meet all program requirements *at the time of validation* (i.e., was not voluntarily provided, was of a type customarily in the public domain, or was subsequently determined to be false). Under such circumstances, the PCII PM will review the submission's validation status.

The submitter may also, at any time after submission of CII and for any reason, request in writing that his or her submitted information no longer be protected as PCII.

In the event that the PCII PM determines that the information should not retain its PCII protection or the submitter requests that his or her submitted information no longer be protected as PCII, the PCII Program Office will:

- Notify the submitter of the change in status
- Remove the PCII markings from the information
- Change the designation of the information in PCIIMS
- Notify users of the information of the change in status.

If there is no indication that the information has been used as PCII, the PCII Program Office will notify the submitter of the change in status and ask him or her to specify whether the information should be destroyed or retained without protection under the CII Act. If the PCII Program Office does not receive a response to this request within 30 calendar days of notifying the submitter of the change in status, the PCII Program Office may retain the information without protection or destroy it in a manner consistent with the appropriate National Archives and Records Administration-approved records disposition schedule. See Section 11, "Destruction of PCII".

5.11 TIME-SENSITIVE PCII AND VALIDATION IN EXIGENT CIRCUMSTANCES

Time-sensitive submissions may be given priority in the validation process. Depending on the timeframe involved and the criticality of the information, certain validation procedures may be waived or shortened with the permission of the PCII PM, as long as the validation process still ensures that a submission meets the requirements for PCII protection before it is validated.

In exigent circumstances, as defined in Appendix 2, "Definitions", the PCII Program Office recognizes that there may be situations in which CII has to be validated as PCII and disseminated on an emergency basis. In such instances, as long as the submitter requests the protections of the CII Act and the CII is given to a Federal employee, the information will have the presumption of protection and be considered as undergoing the validation process. Once the exigent circumstances have subsided, the PCII Program Office will undertake the standard validation process (see Section 5, "Validation"). The PCII Program Office will validate the information and mark it as PCII if it meets the criteria of the CII Act. If the CII does not meet the validation criteria, the Program Office will return it or destroy it based on the submitter's instructions.

5.12 VALIDATION OF ORALLY SUBMITTED INFORMATION

Information may be submitted orally to the PCII Program provided that a similar written statement memorializing the nature of the oral submission is submitted within a reasonable period of time (15 calendar days) following the oral communication. This written statement must include an Express Statement and a complete Certification Statement. Oral submissions will not be entered into the PCIIMS or validated until the written statement is received by the PCII Program Office. Upon receipt of the written statement, validation of the oral submission will be the same as for any other submission. Once an oral submission is validated as PCII, the original record of that submission will be destroyed.

5.13 QUALITY ASSURANCE OF THE VALIDATION PROCESS

To ensure consistency in the validation process, the PCII PM is the ultimate arbiter of validation decisions. There is an audit process to ensure that submissions received as part of a categorical inclusion meet the standards necessary to qualify for PCII protection. More information about the categorical inclusion auditing process can be found in Section 12.2.3, "Site Visits and System Audits".

6. MARKING

This section provides procedures for the marking of PCII. To ensure appropriate protections are afforded to PCII, all forms of PCII must be sufficiently marked to alert users to their status and protection requirements. The guidance set forth in this section implements, in part, the direction in the Regulation, Section 29.6, "Acknowledgment of Receipt, Validation, and Marking".

Information submitted to the PCII Program with the Express Statement will carry the presumption of PCII protection until determined otherwise through the validation process (see also Section 5, "Validation"). The PCII Program Office or the Designee must mark such information immediately upon receipt in accordance with PCII Program Office marking requirements. The marking will remain until the PCII Program Office determines that the information no longer qualifies for PCII protection or the submitter requests that the protection be removed.

6.1 PAPER DOCUMENTS

All paper documents containing PCII must be marked with an Identification Number, consistent with the scheme detailed in Section 6.1.1, "PCII Identification Number", and obtained when the information is entered into the PCIIMS. In the case of categorically included PCII, the PCII Program Office will provide an Identification Number scheme to the responsible Designee, as set forth in Section 6.1.1, "PCII Identification Number". There is a space on the PCII Cover Sheet in which the Identification Number for that submission should be placed.

All paper documents containing PCII must also be marked with the prescribed Protection Statement (see Section 6.1.2, "Prescribed PCII Protection Statement"). All paper documents must also have the PCII Cover Sheet affixed to the front of the document (see Section 6.4, "PCII Cover Sheet").

6.1.1 PCII Identification Number

Upon receipt by the PCII Program Office, all submissions will be entered into the PCIIMS, which will assign the submission an Identification Number using the following format:

PCII-PCIIPO-[State Postal Code of submitting entity]-[Numeric Sequence]-[Update Version]

For submissions made to Designees under a categorical inclusion, a PCII Identification Number will be given to each submission and will consist of two components. The PCII Program Office assigns the *first component*. The Designee automatically generates the *second component*, which will be unique for each submission. The first component will be in the following format:

PCII-[Project Acronym]

The Designee will use the following format for assigning the second component of the Identification Number:

[State Postal Code of submitting entity]-[Numeric Sequence]-[Update Version]

The following is an example of the Identification Number that would be assigned to a submission from Louisiana regarding the Buffer Zone Protection Program:

PCII-BZPP-LA-000001

6.1.2 Prescribed PCII Protection Statement

All PCII materials, or the cases or containers in which they are stored, must be labeled with the following statement:

> This document contains Protected Critical Infrastructure Information (PCII). In accordance with the provisions of the Critical Infrastructure Information Act, 6 U.S.C. §§ 131 *et seq.*, it is exempt from release under the Freedom of Information Act (5 U.S.C. § 552) and similar State and local disclosure laws. Unauthorized release may result in criminal and administrative penalties. It is to be safeguarded and disseminated in accordance with the Critical Infrastructure Information Act, 6 U.S.C. §§ 131 *et seq.*, the implementing Regulation, 6 C.F.R. Part 29 and PCII Program requirements.

6.1.3 PCII Program Office Marking Requirements

After being validated as PCII, all submissions must be marked in accordance with PCII Program Office marking requirements. Any work products containing PCII must be similarly marked.

Original or Copies of Original PCII

The first page of all original PCII or copies of original PCII must feature the PCII Protection Statement described in Section 6.1.2, "Prescribed PCII Protection Statement", in a location that does not obscure the existing information.

All pages of such a document must feature the following notation in the header and footer:

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

In addition, the Identification Number for the information must be placed in the footer of the page(s) on which the information appears.

Work Products Containing PCII

The first page of all PCII derivative products must feature the following:

- The PCII Protection Statement described in Section 6.1.2, "Prescribed PCII Protection Statement", in a location that does not obscure the existing information
- The following notation in the header and footer:

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

- The Identification Numbers of all PCII used in the creation of the derivative product, placed in the page's footer.

Any page containing PCII within a derivative product must feature the following notation in the header and footer:

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

The footer of each page of a derivative product must also contain the relevant Identification Numbers for all PCII used on that page.

PCII commingled with classified information must comply with all marking requirements of both PCII and the highest level of classification with which it is commingled, as prescribed in Executive Order 12958, as amended, and its implementing directives. For more guidance on marking PCII derivative products, consult the PCII Program's *Guide for PCII Work Products* (Appendix 8).

6.2 PCII RECEIVED OR ACCESSED ELECTRONICALLY

Electronic submissions, electronic information in the PCIIMS and other databases, and electronic copies of PCII must have a marking to identify them as PCII. The marking will include the Protection Statement, described in Section 6.1.2, "Prescribed PCII Protection Statement", to ensure users are aware that they are accessing and handling PCII. In these instances, the PCII Program Office will work with the administrators of systems on which PCII can be accessed to provide adequate markings, described in this section, that alert the user that he or she is viewing PCII.

The system must display on the first screen that contains PCII the Protection Statement described in Section 6.1.2, "Prescribed PCII Protection Statement". The statement may appear as a pop-up box, hyperlink, mouse-over, or in other similar methods that ensure the user reads the statement when PCII viewing begins. The system must also display the Identification Number(s) relevant to the document or record being viewed.

The system must, at all times when PCII is visible, display a warning banner on the top of the work space. This banner must remain at the top of the screen even if the viewer scrolls within a file. The following is an example of an acceptable banner:

**********WARNING**********
PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

If the system allows the user to export or print a file contained on the system, the administrator must coordinate with the PCII Program Office to ensure that the resulting printout or exported file has the appropriate PCII markings, including the PCII Cover Sheet.

6.3 PCII IN VIDEO OR AUDIO FORMAT

Some physical or electronic formats present certain challenges to the standard marking requirements. In such cases, alternative approaches will be taken for attaching the Protection Statement described in Section 6.1.2, "Prescribed PCII Protection Statement", and associating information with its Identification Number. In most cases, neither the PCII Program Office nor the Designee will have the resources to edit video or audio files in order to include in them a

warning statement or banner alerting users that the file contains PCII. The PCII Program Office or Designee will instead provide physical markings to the container or case holding the file.

If a video or audio file is received electronically, the PCII Program Office or Designee must transfer the file to an appropriate physical medium (i.e., CD, flash drive, magnetic tape). After the transfer, the recipient must affix the following banner to the physical medium:

WARNING: PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

The PCII Program Office or Designee must also label the physical medium containing the video or audio file with the PCII Protection Statement described in Section 6.1.2, "Prescribed PCII Protection Statement".

The Designee should consult with the PCII Program Office should he or she have any questions about marking these types of files.

6.4 PCII COVER SHEET

The PCII Cover Sheet must be affixed to all physical copies of PCII materials. The Cover Sheet serves as a shield to alert individuals that PCII is attached. All individuals in a PCII work area may be authorized to access PCII, but they may not all have a valid need-to-know for all the PCII materials in the work area. Consequently, PCII materials should always be protected with the Cover Sheet, whether in storage, transit, or on a desk, even if that desk is in an environment where the most rigorous access controls are in place. The PCII Program Cover Sheet can be found in Appendix 9.

The Cover Sheet must—

- Be positioned in such a manner that the PCII cannot be viewed by individuals in the immediate area who are not working with the information
- Remain with PCII materials at all times
- Be placed on top of a transmittal letter or memorandum.

The PCII Cover Sheet must be placed immediately behind a fax transmittal sheet. When the fax is received, the fax transmittal sheet may be removed.

Classified Information

For cases in which PCII is commingled with classified information, the PCII Cover Sheet must be placed immediately behind the classified Cover Sheet required by Executive Order 12958, as amended, Classified National Security Information.

7. SAFEGUARDING PCII

This section sets forth the requirements for safeguarding PCII in accordance with the CII Act, the Regulation (Section 29.7, "Safeguarding of Protected Critical Infrastructure Information"), and applicable DHS Management Directives. The following safeguarding procedures have been established by the PCII PM under the authority of the Regulation to describe the measures required to ensure that information submitted to the PCII Program Office or its Designees and validated as PCII is properly protected throughout its life cycle.

All PCII recipients share responsibility for ensuring that PCII is properly safeguarded in accordance with the policies and procedures promulgated by the PCII Program Office. In particular, Federal government employees who do not follow these safeguarding procedures may be subject to disciplinary action and to the civil and criminal penalties set forth in the CII Act. In addition, State and local governments receiving PCII are required to treat breaches of the safeguarding requirements by their employees or contractors as matters subject to the criminal code or to the applicable employee code of conduct for the jurisdiction.

These safeguarding measures apply to all PCII, including PCII undergoing the validation process.

7.1 GENERAL SAFEGUARDING PRINCIPLES

Although the procedures are intended to be thorough, there may be situations for which the procedures may not provide explicit guidance. In those instances, individuals with access to information submitted to the PCII Program Office are expected to—

- Ensure that their actions are consistent with the principles and guidelines set forth in the CII Act; the Regulation; applicable guidance documents; and guidance from a supervisor, a PCII Officer, the Designee, and/or the PCII PM; and
- Notify a supervisor, a PCII Officer, and/or the PCII PM of any procedures that are incomplete or ambiguous so that they can be augmented or clarified.

In general, safeguarding measures must ensure that—

- Precautions are taken to prevent unauthorized persons from overhearing conversations, observing PCII materials, or otherwise obtaining such information
- PCII is accessed only by authorized users
- To the extent feasible, submitted information is not at risk of inappropriate use
- PCII is not disseminated inappropriately.

7.2 PROCEDURES FOR SAFEGUARDING PCII

Recipients of PCII, including copies of PCII and derivative work products, must safeguard the PCII to ensure that PCII is—

- Accessed by authorized users who are properly trained in how to handle PCII, and
- Safeguarded in accordance with all the guidance from the PCII PM.

The PCII Officer within a given entity is responsible for ensuring that all PCII held by his or her organization is properly safeguarded in accordance with all guidance from the PCII PM.

Generally, original PCII and copies of PCII are subject to the same safeguarding measures. DHS components and Federal agencies designated to receive categorically included PCII must meet the same requirements for storage as those implemented by the PCII Program Office for storage of original PCII. All sites or databases that store original PCII are considered part of the PCII Program's distributed framework. See Section 7.4, "Distributed Data Framework".

To ensure the proper safeguarding of PCII, the PCII PM (for the PCII Program Office), or the PCII Officer (for entities or agencies other than the PCII Program Office) must ensure that the following storage and handling requirements are met:

- Controls limit access to physical storage locations to those individuals explicitly authorized to access PCII.
- Copiers, shredders, and printers in the storage location are only accessed by authorized users.
  - Copy machine (this includes fax machines and any other machines used to make copies) and printer malfunctions must be cleared after use and all paper paths checked for PCII and all unusable pages must be shredded immediately.
  - Copy machines, fax machines, scanners, and similar equipment used to transmit or copy PCII that store copies in memory must have their memories cleaned before either allowing vendor personnel to access such machines for repair or maintenance or disposing of such machines.

- PCII is physically stored in lockable containers or cabinets. These storage containers must be located in a restricted access location preventing access by unauthorized persons. PCII may not be stored in a container with valuables, such as cash, but PCII can be stored in a container with classified information. In the absence of lockable containers or cabinets, PCII is stored in a room or area that has sufficient physical access control measures to offer adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know. Examples include a locked room or an area where access is controlled by a guard, a cipher lock, or card reader.

- The PCII Officer or Designee or a senior official with the authority to commit the government entity must sign an ATO that defines the requirements for safeguarding original PCII on an electronic database. Failure to abide by the terms of the agreement may result in all held PCII being removed from the government entity and stored at the PCII Program Office.

- Systems and computer work stations must meet the system requirements set forth in the terms of the SRD to which the government entity agreed.

- Computer work stations must be configured to allow only authorized users to access electronic databases used for storage of PCII.

- Directions must be provided for logging the access and return of PCII, as applicable.

- Electronic databases storing PCII must have the appropriate firewalls with anti-virus and anti-spyware software installed to prevent unauthorized access.

Any electronic databases storing original PCII must be backed up according to appropriate SOPs and to the requirements set forth in Table 7-1, Backup Requirements. All tape backups containing PCII must be marked as "Protected Critical Infrastructure Information" and must be stored in a secure location. Furthermore, a list of all individuals with physical and virtual access to the system backups must be furnished to the PCII Program Office. Any updates to this access list must be communicated to the PCII Program Office. If backups are stored offsite for continuity of operations, then the name and address of the storage location must be provided to the PCII Program Office.

Table 7-1. Backup Requirements

Requirements for Backing Up Systems Containing Original PCII
The system must back up PCII. The backup schedule/scheme must have the capability to restore the system to the last known good state. There is no requirement to retain outdated versions of PCII submissions. All backups must be stored in a secure location. The PCII Program Office must review and approve the backup scheme. Outdated tape backups may be destroyed or erased when a newer update is created. NOTE: Data backups of PCII may be commingled with non-PCII data on the same medium. However, these backups must be marked and handled as PCII. For systems containing both classified information and PCII, system backups must conform to classified information requirements as well as to PCII procedures. All physical copies of backups containing PCII data must be marked with the following: Protected Critical Infrastructure Information This (insert appropriate media name [i.e., backup tape, disc, etc.]) contains Protected Critical Infrastructure Information (PCII). In accordance with 6 U.S.C. §§ 131 *et seq.* – The Critical Infrastructure Information Act of 2002 (CII Act) and the implementing Regulation at 6 C.F.R. Part 29, the PCII is exempt from release under the Freedom of Information Act (5 U.S.C. 552), State or local disclosure laws and use in civil litigation proceedings. Unauthorized release may result in civil penalty, imprisonment or other action. Safeguard PCII from unauthorized disclosure. The following statement must be entered in the backup job description: Information on this backup job may contain Protected Critical Infrastructure Information.

Any system or database containing PCII must audit all user access to PCII data. Audit data must include at a minimum—

- User name
- User role
- Date and time of access
- Data accessed.

Electronic databases must prevent any change to PCII other than to create a PCII work product or when authorized by the submitter or the PCII PM.

Electronic databases will comply with the *DHS Sensitive System Policy*, Publication 4300A, and the National Institute of Standards and Technology (NIST) standards for sensitive but

unclassified information. Additional information can be found in various NIST Special Publications (e.g., 800-18, 800-26, 800-34, 800-37, 800-50, 800-53), Federal Information Processing Standards (FIPS) (e.g., FIPS 199).

7.3 TRANSMITTING PCII

This section provides guidance on how to safely transmit PCII under normal circumstances. Under exigent circumstances information should be exchanged by approved methods or whatever methods are appropriate to the circumstance.

7.3.1 Mailing

PCII may be mailed using an inter-office service, United States Postal Service First Class, or commercial carriers. PCII sent by mail must be packaged according to these steps:

1. Place a Cover Sheet on any paper documents. Appropriately mark other media such as compact disks. Ensure the Identification Number is visible.
2. Place the PCII in an opaque, tamper-resistant envelope or package, sufficiently sealed to prevent inadvertent opening and to show evidence of tampering.
3. Mark the outside of the envelope or package on all sides with a statement similar to— "STOP! Document contains Protected Critical Infrastructure Information. Only authorized individuals may have access. If you are not authorized to view this information return to the sender or contact the PCII Program Office at 202-360-3023."
4. Place this package into a second outer envelope. Do not identify the package as PCII. The envelope must bear the complete name and address of the intended recipient, who must be authorized to access PCII. Place instructions on the outer envelope stating that if the intended recipient is not available at the address, the package must be returned to the sender. Tracking the departure and receipt of the package is also required.

7.3.2 Wireline Telecommunications and Faxes

Authorized users may exchange PCII via telecommunications only if both parties are in a restricted space that prevents unauthorized disclosure of the information. This applies to conversations conducted over telephone and fax transmissions. Encryption is not required when PCII is discussed over wireline telecommunications networks or when transmitted via fax.

Telephone

1. The person initiating the call must be located in a space that prevents unauthorized disclosure and in which the conversation cannot be overheard by unauthorized users.
2. After making contact, the person initiating the call will confirm that the person on the other end of the line is also located in a space that prevents unauthorized disclosure.
3. Before sharing PCII, alert the potential recipient so that he or she understands what must be protected and how it must be protected.

4. Confirm with the recipient that any notes related to the PCII must be protected and the notes should be appropriately marked to include the Identification Numbers associated with the PCII that was discussed.

Faxes

Faxes may be transmitted via wireline telecommunications and should terminate at another fax machine, rather than a computer or other device. The PCII Cover Sheet must be placed immediately behind a fax transmittal sheet. When the fax is received, the fax transmittal sheet may be removed.

An individual authorized to access PCII must be standing by the destination fax machine to receive the information unless the machine is in an area where access to it is controlled. The sender must contact recipients before faxing PCII and instruct them to acknowledge receipt to the sender.

7.3.3 Wireless Telecommunications: Internet or High Frequency or Other Radio Signal (including Cellular Telephone)

Encryption is required using any encryption method available to both the transmitter of PCII and the PCII recipient. In the event that operational pressures or exigent circumstances make such encryption impossible this requirement may be relaxed. However, the absence of encryption capability does not justify routine unencrypted transmission of PCII via wireless technology.

7.3.4 E-Mail

PCII transmitted via e-mail should be protected by encryption or transmitted within secure communications systems. When this is impractical or unavailable, PCII may be transmitted over non-secured e-mail accounts. For added security, when transmitting PCII over a non-secured e-mail channel, the information should be transmitted as a password-protected attachment, with the password provided under a separate cover. Table 7-2 provides guidance on how to password-protect documents.

Table 7-2. Password-Protecting Documents

To Password-Protect Documents
Instructions for Password-Protecting a Microsoft WORD Document: • Click on the "Tools" icon and click on "Options" • Click on the Security Tab and place cursor in box for "Password To Open" • Type your chosen password in that box • Place a checkmark in the box by "Read Only Recommended" and click "OK" • A screen titled "Confirm Password" will pop up. Retype password and click "OK" • Your document is now password protected
Instructions for Password-Protecting Microsoft PowerPoint Documents: • Click on the "Tools" icon and click on "Options" • Click on the Security Tab and place cursor in box for "Password To Open" • Type your chosen password in that box • A screen titled "Confirm Password" will pop up. Retype password and click "OK" • Your document is now password-protected
Instructions for Password-Protecting WinZip Files • Open the WinZip folder

To Password-Protect Documents
• Click on the "Encrypt" icon • Type your chosen password in both boxes • Your WinZip file is now password-protected
Instructions for Password-Protecting Microsoft Excel Files • Click on the "Tools" icon and click on "Options" • Click on the Security Tab and place cursor in box for "Password To Open" • Type your chosen password in that box • Place a checkmark in the box by "Read Only Recommended" and click "OK" • A screen titled "Confirm Password" will pop up. Retype password and click "OK" • Your document is now password-protected

When sending PCII via e-mail, users must send it as an e-mail attachment and should not place information validated as PCII in the text or subject line of an e-mail.

Senders should:

- Confirm that all recipients have homeland security duties and a valid need-to-know
- Compose e-mail to recipients
- Enter "This E-mail Contains Protected Critical Infrastructure Information (PCII)" into the subject line of the e-mail
- Enter the standard PCII language in Table 7-3 below into the body of the e-mail.

Table 7-3. Standard PCII E-Mail Language

Standard PCII E-Mail Language
********* THIS E-MAIL CONTAINS Protected Critical Infrastructure Information (PCII) ********* You have received this e-mail because the sender believes that you have homeland security duties and have a need-to-know the attached information. If you are not currently a PCII Authorized User, you must send an e-mail to PCII-Training@dhs.gov to request a brief training course within 30 calendar days of the receipt of this e-mail. Attention Non-Federal employees: The attached document contains PCII. By clicking on the attached document, you acknowledge the following: By reviewing this e-mail and accepting the attached PCII you are agreeing not to disclose it to other individuals without following the access requirements and to abide by the guidance contained herein. Your acceptance provides immediate access only to the attached PCII. **You will comply with all requirements summarized below and also found in 6 U.S.C. § 131 *et seq.* – The Critical Infrastructure Information Act of 2002 (the CII Act), the implementing regulation – 6 C.F.R. Part 29, as amended (the Regulation), and the applicable PCII Procedures Manual, as amended, and with any such requirements that may be communicated to you by the PCII Program Manager or PCII Program Manager's designees.** This document contains PCII. In accordance with the provisions of the CII Act, it is exempt from release under the Freedom of Information Act (5 U.S.C. 552) and similar State and local disclosure laws. Unauthorized release may result in criminal and administrative penalties. It is to be safeguarded and disseminated in accordance with the CII Act, the Regulation, and PCII Program requirements. **PCII can only be shared with individuals who have homeland security duties and a need-to-know.**

Standard PCII E-Mail Language
Storage: When not in your possession, store in a secure environment such as a locked desk drawer or locked container. Do not leave the document unattended. Transmission: **Hand Delivery:** Authorized individuals may hand carry material as long as access to the material is controlled while in transit. **E-mail:** Encryption should be used. However, when this is impractical or unavailable, you may transmit PCII over regular e-mail channels. If encryption is not available, send PCII as a password-protected attachment and provide the password under separate cover. Do not send PCII to personal, non-employment related e-mail accounts. Whenever the recipient forwards or disseminates PCII via e-mail, place that information in an attachment. **Mail:** USPS First Class mail or commercial equivalent. Place in an opaque envelope or container, sufficiently sealed to prevent inadvertent opening and to show evidence of tampering, and then placed in a second envelope that has no marking on it to identify the contents as PCII. Envelope or container must bear the complete name and address of the sender and addressee. Envelope will have no outer markings that indicate the contents are PCII and must bear the following below the return address: "POSTMASTER: DO NOT FORWARD. RETURN TO SENDER." Adhere to aforementioned requirements for interoffice mail. **Fax:** You are encouraged, but not required, to use a secure fax. When sending via non-secure fax, coordinate with the recipient to ensure that the faxed materials will not be left unattended or subjected to unauthorized disclosure on the receiving end. **Telephone:** You are encouraged to use a Secure Telephone Unit/Equipment. Use cellular phones to discuss PCII only in exigent circumstances. **Reproduction:** Ensure that a copy of the Cover Sheet is the first page of all reproductions containing PCII. Clear copy machine malfunctions and ensure all paper paths are checked for PCII. Destroy all unusable pages immediately. **Destruction:** Destroy (i.e., shred or burn) the attached document containing PCII when no longer needed. For PCII on laptops or CPUs, delete file and empty recycle bin. For more information on PCII safeguarding and handling requirements, go to www.dhs.gov/pcii. ********** THIS E-MAIL CONTAINS PCII **********

- Attach PCII document to e-mail as an e-mail attachment
- Check correct typing of all e-mail addresses
- Send e-mail to recipients.

7.3.5 Automated Information Systems

All Automated Information Systems (AIS) or AIS networks used to handle, store, or transmit PCII must have operational and technical controls in place to ensure that only authorized personnel and processes can access electronic PCII. A Federal entity's Chief Information Officer must certify and accredit for operations any AIS containing PCII in accordance with Federal and DHS standards. Consult *DHS Information Technology (IT) Security Handbook for Sensitive Systems*, Publication 4300A for additional guidance. A copy of the certification and accreditation should be sent to the PCII Program Office.

State and local government entities are required to have commensurate security measures in place. This includes securing the operating environment, implementing rigorous identification and authentication measures, and establishing access controls that enforce security policy and limit access privileges to the minimum access required to fulfill authorized job responsibilities.

7.4 DISTRIBUTED DATA FRAMEWORK

The PCII Program Office uses a distributed data framework for the receipt, storage, and dissemination of original and copies of PCII. As part of the distributed data framework, PCII and copies of PCII are stored on different systems:

- Original CII submitted to the PCII Program Office is maintained on the PCII Program Office's own PCII repository.
- Original CII submitted to a Designee as part of a categorical inclusion is maintained on a Federally-owned and managed system for which the recipient Designee is responsible. Such systems may also maintain copies of PCII.
- Copies of PCII may be stored on systems owned by accredited State or local government entities. The PCII Officer for each such entity is responsible for the PCII stored on these systems.

Each Designee is responsible for the receipt and marking of original PCII submitted as part of a categorical inclusion, as well as for facilitating access to the PCII repository in which these submissions are stored. The PCII Officer or Designee is responsible for ensuring that the initial dissemination of PCII from a Federally-owned and managed repository be tracked. A PCII Officer will be responsible for overseeing the use of PCII once it is disseminated beyond the original PCII repository. In order to facilitate the sharing of PCII stored on multiple, geographically dispersed systems that make up the distributed data framework, the PCIIMS maintains a defined set of metadata for all original PCII on every system within the framework.

To access repositories that are part of the distributed framework, an authorized user must be an account holder for the specified repository or be given permission to access the repository. The catalog of PCII generated by the PCIIMS and distributed regularly to authorized users will notify them where PCII is located. If a PCII catalog entry indicates that the PCII is stored in a repository for which the user does not have an account, the user should contact the administrator or system owner of the repository and request access to the specific PCII. Should the repository owner or administrator determine that the user does not have a valid need-to-know and deny the user access to the PCII, the user should contact the PCII Program Office directly.

7.5 TRAVEL AND TEMPORARY DUTY STATIONS

In general, PCII should not be removed from an accredited entity's protected facilities. However, if it is necessary to travel with PCII documents, additional safeguard measures must be taken. In general, PCII should be safeguarded using the same general principles applicable to safeguarding a cell phone, laptop, or other personal electronic device (e.g., it should not be unattended in public places).

If traveling with documents containing both PCII and classified information, the travel requirements specified in Executive Order 12958, as amended, Classified National Security Information, and its implementing directives must be followed.

The following describes the measures required to protect PCII while traveling. If there is an actual or suspected compromise of PCII, the procedures described in Section 12.3, "Violations of PCII Procedures", should be followed.

In All Cases

- PCII must be under the control of an authorized user at all times.
- When not in use, PCII must always be placed in an opaque envelope and double wrapped when traveling. See Section 7.3.1, "Mailing", for further information on double wrapping PCII.
- PCII and PCII-derived materials must always have a Cover Sheet attached and the materials must not be displayed when PCII is not used.
- Information identifying the submitter is PCII and must be protected accordingly.

While in Transit

- PCII may not be openly viewed in a public place.
- PCII must be hand-carried when using public transportation (it may not be put in checked luggage) and the traveler must remain in possession of PCII at all times (e.g., take it with them to the restroom, dining car, etc.).
- When traveling by car, properly packaged PCII may be locked in the trunk when the traveler is away from the vehicle.

In a Hotel

- If a room safe is available and suitable, it is the preferred method for protecting PCII while in the hotel. Otherwise, take other suitable precautions available to protect PCII from unauthorized individuals and to reveal evidence of tampering. Such precautions may be similar to precautions used for protecting personal valuables while traveling.
- PCII (hard copy or electronic) must not be visible to individuals not authorized to access PCII or without a valid need-to-know for that particular information.

8. ACCESS, DISSEMINATION, AND USE

This section sets forth the procedures for the access, dissemination, and use of PCII and implements Section 29.8 of the Regulation, "Disclosure of Protected Critical Infrastructure Information". PCII authorized users are responsible for ensuring that PCII is used for appropriate purposes and safeguarded and handled in accordance with the procedures set out in the CII Act, the Regulation, these procedures, and any additional guidance promulgated by the PCII PM. The PCII Officer and Designee have additional oversight responsibilities relating to the access, dissemination, and use of PCII.

8.1 PCII ACCESS REQUIREMENTS: REGULAR VS. ONE TIME

Potential PCII users must meet certain standard requirements before they will be granted access to PCII on a regular or one-time basis.

8.1.1 Regular PCII Access Requirements

All PCII users will be assigned a PCII Officer to whom they can turn for answers to any questions. Usually, the PCII Officer is an individual working in the same entity (or State) as the PCII user. The PCII Program Office will act as the PCII Officer for all authorized users assigned to an entity which does not yet have a PCII Officer.

Before accessing PCII, an individual must—

- **Be an Individual Employee or Contractor for a Federal, State, or Local Government Entity.** Members of the private sector, individual citizens, media, trade associations, and other private sector organizations cannot be PCII authorized users.
- **Be Assigned Homeland Security Duties.** All users of PCII must have homeland security duties that are defined, relative to PCII, as duties in support of securing critical infrastructure or protected systems; analysis; warning; interdependency study; recovery; reconstitution; or other appropriate purposes, including without limitation, the identification, analysis, prevention, preemption, and/or disruption of terrorist threats to the homeland.
- **Complete PCII Training.** Prior to accessing PCII, a user must be trained in PCII safeguarding and handling requirements. The most common and preferred method for accomplishing this is having the individual complete the PCII Authorized User Training, which can be obtained by e-mailing the PCII Program Office at PCII-Training@dhs.gov. Under some circumstances, users may complete the PCII Authorized User Training in a classroom setting as part of a project involving PCII. When this is the case, the classroom trainer will be responsible for providing evidence that each individual has successfully completed the training.

  In limited and exigent circumstances, PCII training can be accomplished expeditiously with the PCII Cover Sheet. These steps are outlined in more detail below. Section 9, "PCII Training Program", provides more detail regarding the training requirement.

- **Sign a Non-Disclosure Agreement (Non-Federal Employees Only)**. Prior to accessing PCII, all non-Federal employees must sign a non-disclosure agreement (NDA) (see Appendix 16) as prescribed by the PCII PM. By signing the NDA, the individual attests that he or she is familiar and will comply with all the PCII Program requirements set out in the CII Act, the Regulation, and the PCII Manual and with any requirements that may be communicated to him or her by the PCII Program Office, the Designee, the PCII Officer, or the Deputy PCII Officer.

  This may be accomplished several ways. Users completing the PCII Authorized User Training online electronically sign and submit an NDA. Users completing the PCII Authorized User Training in a classroom setting will have the opportunity to sign an NDA in class, and the classroom trainer will be responsible for forwarding the signed NDAs to the PCII Program Office.

  In limited and exigent circumstances, NDAs can be executed by reviewing the PCII Cover Sheet and the terms contained on it. By accepting the PCII attached to the Cover Sheet, the individual has accepted the non-disclosure terms. These steps are outlined in more detail below

- **Be Certified by the PCII Program Office or the PCII Officer (Contractors only).** Prior to accessing PCII, a contractor must be certified by either the PCII Program Office or a PCII Officer. Before or during participation in the PCII Program, the contractor must agree by contract to adhere to and implement PCII Program requirements. Section 10.5, "Contractor Certification", provides additional detail about contractor certification and the language to incorporate into the contract with the government entity.

- **Have a Valid Need-to-Know.** Any individual accessing PCII must have a need-to-know for that particular PCII. Before disseminating PCII, the holder of PCII must determine whether the prospective recipient has a valid need-to-know the information. Although the determination of whether an individual or an organization has a valid need-to-know is a judgment call made on a case-by-case basis, the determination should be made based on whether the individual has homeland security duties and what the recipient intends to do with the PCII. Section 214 (a) of the CII Act lists the authorized uses of PCII (which includes use of PCII in work products) as—
  - Securing the critical infrastructure and protected systems
  - Analysis
  - Warning
  - Interdependency study
  - Recovery
  - Reconstitution
  - Another informational purpose, including, without limitation, the identification, analysis, prevention, preemption, and/or disruption of terrorist threats to our homeland.

If the recipient intends to use the PCII for regulatory purposes or other purposes that are expressly prohibited in the CII Act and the Regulation, then the recipient does not have a valid need-to-know. The PCII Program Office can provide further guidance on this matter and should be contacted if there are any questions or doubts about the validity of an individual's need-to-know.

Examples of Valid and Invalid Need-to-Know

Mike, an employee for the Transportation Security Administration (TSA), has multiple vulnerability assessments about subway stations across the country. These vulnerability assessments are validated as PCII.

Valid Need-to-Know: Mary, a contractor supporting DHS, is drafting a report on the vulnerabilities of the transportation sector and wants to use Mike's PCII vulnerability assessments. She will use her findings to produce a best-practices guideline for mass-transit security. She intends to share this document with Federal, State, and local law enforcement officials to assist in their security efforts.

Invalid Need-to-Know: Joe is a Federal government employee at TSA. He is drafting a report on the vulnerabilities of the transportation sector and wants to use Mike's PCII vulnerability assessments to support his claim to TSA that regulations should be imposed on train stations.

The Designee; Federal, State, and local government entities; and authorized PCII users may disseminate PCII in their possession provided they ensure that the person to whom they are disseminating PCII meets all the access requirements set forth above. Authorized users must transmit PCII in accordance with the procedures set forth in Section 7.3, "Transmitting PCII".

8.1.2 One-Time PCII Access Requirements

A Federal, State, or local government employee or contractor may require access to PCII before completing PCII Authorized User Training. PCII may be accessed on a one-time expedited basis provided that he or she completes the PCII Authorized User Training within 30 calendar days of such access. By adhering to the following protocols, a holder of PCII can share it with a recipient who has not been previously authorized:

- The holder of PCII confirms that the recipient is a Federal, State, or local government employee or contractor and has homeland security duties.
- The holder of PCII confirms that the recipient has a valid need-to-know.
- The recipient reviews the PCII Cover Sheet and agrees to comply with PCII handling and safeguarding requirements.
- The recipient's acceptance of the PCII Cover Sheet and the accompanying PCII satisfies the NDA requirement for that one-time access to that PCII.
- The recipient completes the PCII Authorized User Training within 30 calendar days of receiving the PCII, by following the instructions on the PCII Cover Sheet.

8.1.2.1 Distributing and Discussing PCII in a Meeting

There may be instances when participants in a meeting will need to discuss PCII. Ideally, all participants will be authorized users and the PCII holder who plans on discussing PCII should confirm this and ensure that all participants meet the requirements set forth in Section 8.1.1,

"Regular PCII Access Requirements". In the event that participants are not authorized PCII users, the holder of the PCII must follow additional procedures to ensure that the participants are authorized on a one-time basis. The protocols below set forth the procedures for ensuring that PCII is properly accessed during meetings.

Pre-Meeting

The PCII holder, in coordination with the organizer of the meeting, must—

- Confirm that all attendees are authorized PCII users and have homeland security duties and a valid need-to-know
- Send an e-mail to all attendees stating that PCII will be disseminated and/or discussed during the meeting
- Instruct non-authorized users to become authorized by completing the PCII Authorized User Training, which can be obtained by e-mailing the PCII Program Office at PCII-Training@dhs.gov
- Ensure that a PCII Cover Sheet is attached to any PCII that will be disseminated during the meeting.

During Meeting

The PCII holder, in coordination with the organizer of the meeting, must—

- Confirm that all attendees have homeland security duties and a valid need-to-know and have completed the PCII Authorized User Training
- Briefly review PCII handling requirements found on the PCII Cover Sheet
- Ensure that all non-Federal government employees sign an NDA before PCII is discussed at the meeting
- Distribute PCII
- Instruct non-authorized individuals to become authorized by completing, within 30 calendar days of the meeting, the PCII Authorized User Training, which can be obtained by e-mailing the PCII Program Office at PCII-Training@dhs.gov .

These protocols will allow a non-authorized user to access PCII only during the meeting. For access to PCII on a regular basis, PCII Authorized User Training must be completed.

8.1.3 Background Checks

Section 29.7(b) of the Regulation states that DHS will, to the extent practicable and consistent with the purposes of the CII Act, undertake appropriate background checks to ensure that individuals with access to PCII do not pose a threat to national security. Any inquiries relating to background checks should be forwarded to the PCII Program Office.

8.2 DISSEMINATION

Information submitted for protection under the CII Act may not be disseminated until it has been validated. The PCII Program Office or the Designee is authorized to provide access to PCII when it is determined that this access supports homeland security purposes as set forth in the CII Act. The PCII Program Office or the Designee may provide PCII to Federal departments and

agencies and to State and local government entities that have executed an MOA with the PCII PM and have met the minimum requirements of the PCII Accreditation Program. The PCII PM or the Designee is responsible for tracking PCII initially provided to the Federal, State, or local government entity. See also Section 8.3, "Tracking".

8.2.1 Requested Limited Dissemination PCII

The submitter may request that the information, once validated as PCII, be shared only with specific government entities or individuals. Such limitations, however, do not impact any of the requirements and obligations associated with PCII, including sharing PCII with the Government Accountability Office (GAO) or Congress or supporting the purposes of the CII Act. Requests may not exclude DHS, but may limit access to a specific office or component within the Department. The PCII Program Office or the Designee will cooperate with the submitter to ensure that the PCII is disseminated to the appropriate entities, programs, or individuals. When sharing Requested Limited Dissemination PCII, users must take the extra step of ensuring that all recipients are employees of the organizations identified by the submitter.

Circumstances may arise when a user needs to share Requested Limited Dissemination PCII with users who do not work for organizations identified by the submitter. For example, a submitter requests that only the State of Maryland access its PCII but a user who works for the State of Virginia needs access to it in non-exigent circumstances. Although the Maryland PCII authorized user's PCII Officer must notify the submitter before giving access to the Virginia user, the submitter's consent is not a pre-requisite to sharing PCII with the Virginia user. Furthermore, in exigent circumstances, the Maryland PCII Officer may not be able to contact the submitter before sharing the information with the Virginia user.

If, in non-exigent circumstances, the submitter does not give his or her consent, the following procedures should be followed before the information is shared with the Virginia user:

1. The Maryland PCII Officer lets the submitter know that the PCII Program Office is the ultimate arbiter in deciding whether or not the PCII will be shared with the Virginia user.

2. The Maryland PCII Officer contacts the PCII Program Office and notifies the PCII Program Office that Virginia would like access to the requested limited dissemination PCII but that the submitter has not agreed to sharing it with Virginia.

3. The Program Office will make a final determination whether the information should be shared. If the information should be shared, the Program Office will notify the submitter that the information will be shared with the Virginia submitter.

4. The submitter has the option of requesting that the PCII protections be removed. In such instances, the PCII Program Office will change the status of the information and the information will no longer be PCII. Furthermore, the information will be destroyed or returned to the submitter, depending on the submitter's instructions.

5. If the submitter does not request a change in status and that the PCII be destroyed or returned to him or her, the PCII Program Office will direct the Maryland PCII Officer to provide the information to the Virginia user.

After the information has been shared, the Maryland user must contact and inform the submitter of the following:

- What information was shared
- When the information was shared
- With whom it was shared.

The Maryland user must also notify the PCII Program Office that information has been shared with the Virginia user and provide the same information to the PCII Program Office.

The procedures below describe what additional actions the holder must take to share Requested Limited Dissemination PCII with individuals who are outside of the organizations identified by the submitter. When access to Requested Limited Dissemination PCII is expanded, whether in normal or exigent circumstances, the user sharing the PCII must record the expansion as well as the names of individuals with whom PCII was shared and immediately inform the PCII Program Office in writing. The holder of the PCII and/or the PCII Program Office must inform the submitter that the limited dissemination request was expanded.

Procedure

1. The individual holding PCII receives the submitter's written consent to expand access beyond the originally designated recipients. In exigent circumstances, this may not be possible, and the individual should proceed immediately to Step 2.
2. The holder of PCII shares it with the requester.
3. The individual who shared the PCII creates a record that includes the Identification Number, the date that information was shared, and the recipient's name and contact information.
4. The individual who shared the PCII retains the original record of the dissemination log and sends a copy to the PCII Program Office and the Designee. In the absence of a Designee, the PCII should be sent to the PCII Officer.
5. The PCII Program Office updates the PCIIMS to indicate that additional users may access the Requested Limited Dissemination.

8.2.2 Further Dissemination by Federal, State, and Local Government Entities

The Designee or PCII Officers or authorized users in Federal, State, and local government entities other than the PCII Program Office may disseminate PCII in their possession provided they—

- Verify the individual is an authorized user and meets the requirements set forth in Section 8.1.1, "Regular PCII Access Requirements"
- Encourage the recipient to track the information as he or she shares and disseminates it.

If Federal government employees and contractors want to share PCII with unauthorized users, the users must become authorized or the employee must obtain the express approval of the PCII PM or the Designee to share the PCII with an unauthorized user.

8.2.3 Further Dissemination by State and Local Government Entities to Users not Previously Authorized by the PCII PM or the Designee

State and local government employees and contractors receiving PCII may not share it with any parties that have not been authorized by the PCII PM or the Designee. If State and local government employees and contractors want to share PCII with unauthorized users, the users must become authorized or the employee must obtain the express approval of the PCII PM or the Designee to share the PCII with an unauthorized user. The PCII PM generally will not grant such approval without the written consent of the submitter.

8.2.4 Dissemination Requiring Written Consent of the Submitter

PCII may not be used directly by DHS or other Federal authority; State or local authority; or a third party in any civil action arising under Federal or State law, without first obtaining the submitter's written consent to do so. Such consent is required for each request individually.

Only the PCII PM or a Designee may seek and obtain written consent from persons or entities submitting information when such consent is required under the CII Act to permit disclosure. In all circumstances, State and local recipient entities must go through the PCII Program Office or a Designee to seek the submitter's consent to disclose PCII when such consent is required under the CII Act.

Only in exigent circumstances, and upon contemporaneous notice to the PCII PM, may any Federal government employee whose entity is participating in the PCII Program contact submitters directly to seek their consent to the disclosure of PCII when such consent is required under the CII Act.

8.3 TRACKING

PCII must be tracked under specified circumstances. The section below sets forth the details of the tracking process.

Who

The PCII Program Office or Designee must track the access and dissemination of original PCII when it is disseminated from an original PCII repository. The PCII Program Office must track the initial dissemination of PCII held by the PCII Program Office to an authorized user. Likewise, the Designee is responsible for overseeing the tracking of the dissemination of information from the original repository he or she manages. Thereafter, authorized users are encouraged, but not required, to record when and to whom they give the information. PCII contained in a system-based repository such as a database, must be tracked when it is received, disseminated, downloaded, and destroyed.

What

The PCII Program Office or Designee must record the following information:

- Identification Number of the PCII
- Date the information was shared

- Name of the recipient and of his or her organization
- Contact information of recipient
- Method by which PCII was provided to the recipient.

Whether the information is logged manually or by a system, the log must capture the five elements listed above.

How

If the information is disseminated from an original PCII repository to an individual (as opposed to a system), the Designee should ensure that the tracking records are current and accurate. If an information system holds and disseminates PCII, the system must have the capability of recording and maintaining the tracking information. The tracking records must be kept until the related PCII is deleted or when the PCII Program Office or the relevant government entity determines that the tracking records are no longer needed for administrative, legal, audit or other operational purposes, whichever is later. The PCII Program Office or the PCII Officer will conduct inspections periodically to ensure that the procedures for tracking are properly followed.

8.4 USE OF PCII IN CIVIL LITIGATION/PCII IN THE HANDS OF THE SUBMITTER

When CII is submitted and validated as PCII, the information and documents provided, and drafts and copies retained by the submitter or person working with the submitter, as well as any discussion with DHS regarding the CII, are considered PCII and cannot be the subject of civil discovery or other direct use in any civil litigation without the submitter's consent. "Civil litigation" includes civil litigation in any form or forum, whether or not the United States, its agencies, officers, or employees is or are parties to such proceedings. Although PCII, including the submitted opinions, evaluations, conclusions, or analyses, 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 be used for such purposes.

8.5 DISSEMINATION TO LAW ENFORCEMENT AGENCIES, CONGRESS, AND THE COMPTROLLER GENERAL

The CII Act and the Regulation require the PCII Program Office to release any PCII to the parties listed below upon their request—

- Law enforcement agencies in furtherance of the investigation or prosecution of a criminal act
- 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
- The Comptroller General, or any authorized representative of the Comptroller General, in the course of the performance of the duties of the GAO

In addition, PCII may be provided to the DHS Inspector General.

The PCII Program Office will not release PCII under these circumstances without taking measures to ensure that the individuals who receive PCII are authorized to receive it and are

properly trained in its protection and use. In particular, with respect to Congressional access to PCII:

- The PCII Program Office will work with the DHS Office of Legislative and Intergovernmental Affairs to confirm that the request is being made by a Member of Congress in their capacity as a member of a congressional committee, as required by the CII Act.
- If the staffer making the request on behalf of the Member of Congress has not previously received Authorized User training, the Program Office will provide computer-based training before the specific PCII will be released.
- As Federal employees, congressional staff will not be required to sign the Non-Disclosure Agreement. Rather, they will sign an Acknowledgement of Roles and Responsibilities (see Appendix 13) with respect to handling, using, and safeguarding PCII.
- The congressional Authorized Users will agree to acknowledge receipt of PCII by signing a Receipt of Record form (see Appendix 13). The receipt must include the identification number of the PCII. Furthermore, the Authorized User will require any person to whom he or she gives PCII to similarly acknowledge receipt of the PCII and retain a copy of that record.

With respect to GAO access to PCII:

- The PCII Program Office will work with the DHS GAO/IG Liaison Office to confirm that the request is being made by GAO and to coordinate the response to the request.
- If the GAO staff potentially accessing PCII has not previously received Authorized User training, the Program Office will provide computer-based training before the specific PCII will be released.
- As Federal employees, GAO staff will not be required to sign the Non-Disclosure Agreement.
- The PCII Program Office will work to assist GAO in implementing PCII safeguarding and handling requirements

If Congress, the Comptroller General, or the DHS IG request PCII directly from a PCII Officer, Designee, or an authorized user, these individuals should (1) adhere to the procedures set forth above, (2) notify the PCII Program Office immediately of such a request and (3) provide the PCII Program Office, in the case of a Congressional request, signed copies of the Acknowledgement of Roles and Responsibilities and the Receipt of Record. The PCII PM will inform DHS' Office of Legislative and Intergovernmental Affairs of any congressional requests or the DHS GAO/IG Liaison Office of any GAO requests for PCII.

8.6 REQUESTS FROM NON-ELIGIBLE ENTITIES AND FROM MEDIA

The general public, ISAOs, and foreign governments may receive advisories, alerts, and warnings prepared from PCII provided these products do not contain any information identifying the submitters of PCII or any proprietary, business-sensitive, or trade secret information. The general public, ISAOs, and foreign governments may *not* receive PCII itself, without the written consent of the submitter. See Section 8.8, "PCII Work Products", for further information on advisories, alerts, or warnings.

PCII-related inquiries from the media must be directed to the accredited entity's or user's PCII Officer. The PCII Officer is encouraged to refer individuals to the PCII Web site for answers to routine inquiries (e.g., submission requirements). Responses to substantive inquiries from the media must be coordinated with the PCII Program Office.

8.7 RESPONDING TO INFORMATION REQUESTS UNDER DISCLOSURE LAWS

PCII is exempt from disclosure under FOIA and other similar State and local disclosure laws. Any participating entity with questions regarding the protection of PCII from public disclosure may contact the PCII Program Office.

Should a request be made under FOIA for PCII (or a request for information under similar State and local laws), participants in the PCII Program must ensure that such requests are handled as follows:

- **State and Local Participating Entities.** PCII Officers must ensure that their respective Disclosure Officers are aware that PCII is Federal information so that they are prepared to make an appropriate response to requests for PCII under their respective disclosure laws. Should a State or local entity receive a request to disclose PCII pursuant to a request under State or local disclosure laws, the PCII Officer should contact the PCII Program Office immediately. The State or local Disclosure Officers must inform requesters that PCII is Federal information and that the CII Act explicitly protects it from disclosure under all disclosure laws. If there are further questions about the applicability of disclosure laws to PCII, State and local participating entities are encouraged to refer the requester directly to the PCII Program Office.
- **Federal Government Participating Entities.** Designees and PCII Officers must refer all FOIA requests for PCII to the DHS Disclosure Officer who supports the PCII Program Office. Any FOIA requests for materials that do not contain PCII must be handled by each Federal entity in accordance with its internal procedures for processing FOIA requests.
- **PCII Program Office.** If the PCII Program Office receives any FOIA requests directly, the PCII PM must refer all such requests to the appropriate DHS Disclosure Officer.

Further, all Designees and PCII Officers are encouraged to—

- Make their respective Federal, State, or local disclosure officers aware of their participation in the PCII Program
- Ensure that such disclosure officers understand the protections afforded PCII from FOIA and State and local disclosure laws
- Develop a process for notifying the Designee or PCII Officer when the Disclosure Officer receives a request for any information protected under the CII Act.

8.8 PCII WORK PRODUCTS

Federal, State, and local government recipient entities may develop two kinds of analytical work products that are derived from PCII: derivative work products and sanitized work products.

Although the PCII Program Office does not create these products, it is responsible for providing guidance to organizations that conduct analysis of PCII with respect to adequately safeguarding PCII under such circumstances. An entity's Designee or PCII Officer is responsible for overseeing the use of PCII in work products. Section 214 (a) of the CII Act and the Regulation list the authorized uses of PCII (which includes use of PCII in work products) as—

- Securing the critical infrastructure and protected systems
- Analysis
- Warning
- Interdependency study
- Recovery
- Reconstitution
- Another informational purpose, including, without limitation, the identification, analysis, prevention, preemption, and/or disruption of terrorist threats to our homeland.

8.9 DERIVATIVE WORK PRODUCTS

Work products containing PCII are subject to the same handling, storage, and marking requirements as original PCII. When work products contain verbatim PCII or anything that explicitly or implicitly refers to the submitter or submitted CII, the work products must be labeled and handled as PCII; otherwise, PCII designation is not required or appropriate. In an unclassified PCII derivative product, only those paragraphs, tables, graphics, and figures containing PCII must be parenthetically marked as PCII. No other paragraphs, tables, graphics, figures, and so on will be portion marked. The Guide for PCII Work Products in Appendix 8 contains additional information relating to the handling and marking of PCII work products.

PCII commingled with classified information must comply with all marking requirements of both PCII and the highest level of classification with which it is commingled, as prescribed in Executive Order 12958, as amended, and its implementing directives. PCII contained in such classified documents retains its PCII marking and does not lose its PCII protection even if the document is subsequently declassified.

When the product does not contain PCII but PCII merely provided insight that led to conclusions or hypotheses, such products can be disseminated as non-PCII.

8.10 SANITIZED ADVISORIES, ALERTS, AND WARNINGS

If Federal, State, or local entities use PCII to prepare advisories, alerts, and warnings regarding potential threats and vulnerabilities to critical infrastructure for dissemination to the private sector, general public, or foreign governments, the entity producing such a derivative product must sanitize it. For the purposes of the PCII Program, "sanitization" means distilling the information so it is not traceable to the submitter and does not reveal any information that—

- Is proprietary, business-sensitive, or trade secret
- Relates specifically to the submitting person or entity (explicitly or implicitly)
- Is otherwise not customarily in the public domain.

Unless exigent circumstances require otherwise, any warning to the general public that is not sanitized in accordance with the directions above must be authorized by the DHS Secretary, the Under Secretary for National Protection and Programs, Assistant Secretary for Cyber Security and Communications, or Assistant Secretary for Infrastructure Protection (ASIP).

Such exigent circumstances exist only when approval of the DHS Secretary, the Under Secretary for National Protection and Programs, Assistant Secretary for Cyber Security and Communications, or the ASIP cannot be obtained within a reasonable time necessary to issue an effective advisory, alert, or warning. The Designee or the PCII Officer must coordinate with the PCII Program Office to issue these warnings in accordance with the Regulation. In issuing advisories, alerts, and warnings, DHS must—

- 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
- 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, any persons or entities on whose behalf the CII was submitted; or is not otherwise appropriately in the public domain.

DHS may consult or cooperate with the submitter in making such advisories, alerts, or warnings. A State or local entity that has submitted its own CII that has been validated as PCII, is not bound to consult DHS in the issuance of an alert, advisory or warning based on such PCII, provided that the State or local entity (a) uses its own copy of the information or (b) has sanitized the warning such that it does not contain any PCII. Otherwise, the State or local entity should follow the procedures set forth above prior to issuing the alert, advisory or warning containing PCII.

9. PCII TRAINING PROGRAM

The PCII Program Office is charged with the receipt, validation, and safeguarding of CII that has been voluntarily submitted to DHS. To ensure the appropriate safeguarding of this sensitive and valuable information, the PCII Program Office requires the successful completion of appropriate training as a condition for granting access to PCII materials.

The PCII Program Office provides training appropriate to the level of participation in the PCII Program, including—

- Training and awareness for authorized users
- Specialized training for PCII Officer and Designee candidates
- Training for the sharing and handling of PCII during exigent circumstances.

9.1 TRAINING AND AWARENESS FOR AUTHORIZED USERS

The PCII Program Office requires that all individuals accessing PCII be trained in the handling and safeguarding requirements for PCII. Accordingly, all Federal, State, or local employees (and their contractors) must complete the PCII Program's Authorized User Training before accessing PCII.

The goal of the PCII Authorized User Training is to ensure that those granted access to PCII are fully trained in the handling and safeguarding procedures provided by the PCII Program Office. The PCII Authorized User Training is available in a self-paced, electronic version that can be e-mailed, upon request, to qualifying individuals with a need to access PCII. Interested parties can obtain the electronic version of the PCII Authorized User Training by contacting the PCII Program Office by phone at 202-360-3023 or by e-mail at pcii-training@dhs.gov.

9.2 PCII OFFICER TRAINING

The goal of the PCII Officer Training is to ensure full familiarity with the CII Act, the Regulation, and procedures and requirements promulgated by the PCII Program, as well as to provide operational knowledge and awareness of PCII Officer responsibilities. To ensure all of these objectives are met, the PCII Officer Training is divided into two parts: pre-work and an instructor-led classroom component.

The pre-work consists of an overview of the PCII Program, a facilitated reading exercise on the CII Act and the Regulation, an interactive Accreditation Process Map, and an assessment of the prospective PCII Officer's understanding of the materials. All pre-work components must be completed before attending the instructor-led component of PCII Officer Training. The pre-work typically takes 2 to 3 hours to complete, in addition to the time required to thoroughly review the PCII Procedures Manual, the CII Act, and the Regulation.

Once a PCII Officer candidate has been nominated by an accredited entity (or an entity seeking accreditation), the PCII Program Office will inform that candidate of the date and location of the PCII Officer Training course and send the pre-work packet described above. The 1-day, instructor-led classroom component of the PCII Officer training consists of an in-depth study of—

- The accreditation process
- The roles and responsibilities of the PCII Officer, Deputy PCII Officer, and Designee
- The means by which PCII must be protected
- Outreach messaging.

The instructor-led component of the training includes a lecture, facilitated discussions, and interactive exercises. PCII Officer candidates must pass a written certification exam when they have completed the training. Upon successful completion of the certification exam, the candidate will be appointed by the PCII PM as his or her entity's PCII Officer.

9.3 DESIGNEE TRAINING

Only Federal employees responsible for a categorical inclusion will be trained as Designees. The goal of the Designee Training is to ensure full familiarity with the CII Act, the Regulation, and procedures and requirements promulgated by the PCII Program, as well as to provide operational knowledge and awareness of Designee roles and responsibilities. To ensure all of these objectives are met, the Designee Training is divided into two parts: pre-work and an instructor-led classroom component.

Once a Designee candidate has been nominated by an accredited entity (or an entity seeking accreditation), the PCII Program Office will inform that candidate of the date and location of the Designee Training course and send the candidate the pre-work packet described above. The 1-day, instructor-led classroom component of the Designee Training consists of an in-depth study of—

- The roles and responsibilities of the Designee
- The means by which PCII must be protected
- Outreach messaging.

The instructor-led component of the Designee Training course includes a lecture, facilitated discussions, and interactive exercises. Designee candidates must pass a written certification exam when they have completed the training. Upon successful completion of the certification exam, the candidate will be appointed by the PCII PM as his or her entity's Designee.

In the event the Designee and the PCII Officer is the same person, he or she will be trained in both roles.

9.4 TRAINING IN EXIGENT CIRCUMSTANCES

In exigent circumstances, as defined in Appendix 2, Definitions, certain PCII handling and safeguarding requirements may be suspended.

If exigent circumstances result in a situation wherein an individual requires one-time access to PCII for a discrete homeland security-related task, the individual is still required to fulfill all PCII access requirements; he or she may be able to do so, however, on an expedited basis. In such circumstances, the PCII Cover Sheet, which is affixed to the top of all PCII, may be used to brief a new, previously unauthorized recipient of PCII on the sensitivity of and handling requirements for PCII.

When the exigent circumstances have subsided, the newly authorized users of PCII should inform the PCII Program Office of the one-time access by sending an e-mail to pcii-training@dhs.gov. If the individual will be accessing PCII on a regular ongoing basis, he or she will still be required to complete the PCII Authorized User Training (and if not a Federal government employee, execute an NDA, which must be provided to the PCII Program Office).

9.5 AUDITING PCII TRAINING COURSES

PCII Program training courses are designed for specific audiences. It is important that participants complete the training appropriate to their role in the program. Occasionally, permission is granted for interested parties to "audit" a course. Typically, this option is offered to allow participants to learn more about the PCII Program in general. When a PCII training course is audited by an interested party, it is possible that the course being audited does not meet all the requirements for his or her level of participation. Some presentations are customized to a particular program and cover specific policies, even exceptions or exemptions. When a course is audited, the interested party is required to contact his or her PCII Officer or the PCII PM to ensure that all requirements for the intended level of participation have been met.

9.6 REFRESHER TRAINING

PCII Officers and Designees will be required to receive refresher training as directed by the Program Office. PCII Authorized Users will receive refresher training on an as-needed basis.

10. ACCREDITATION

The PCII Accreditation Program is designed to provide consistent application of the proper handling, use, dissemination, and safeguarding of PCII by government entities and authorized users. The PCII Accreditation Program allows entities to adapt and construct operational procedures in a format that best meets each entity's needs. The PCII Program Office recognizes that an entity's activity level is likely to depend on its mission, size, structure, population, and specific needs. While all participating entities must demonstrate their ability to meet minimum requirements for handling, using, disseminating, and safeguarding PCII, they can supplement or customize the guidance set forth in this Manual provided they do not dilute the minimum requirements. As an entity's participation in the PCII Program shifts, safeguarding requirements and operational procedures may be adjusted to meet the entity's changing needs. The PCII Program Office is committed to expediting the accreditation of eligible entities. Throughout the process, the PCII Program Office will support all eligible entities in achieving and maintaining accreditation.

10.1 ROLES AND RESPONSIBILITIES

PCII Program stakeholders have the following roles and responsibilities relating to accreditation:

- The PCII Program Office provides accreditation guidance, program oversight, and management to all eligible entities toward achieving and maintaining accreditation.
- Each entity is responsible for the administration and management of the entity's PCII program.
- A senior official within the accredited entity signs the MOA, formalizing the entity's participation in the PCII Program.
- The PCII Officer oversees, administers, and maintains the entity's PCII program.
- Authorized users within the accredited entity must comply with all applicable PCII regulations and procedures.

10.2 ACCREDITATION PROCEDURES

The CII Act, the Regulation, and this Manual establish minimum requirements for accessing PCII. The entity, however, may choose to adapt and customize procedures that are most effective in the entity's environment as long as those procedures ensure compliance with all PCII Program requirements. The accreditation process is designed to ensure that the entity is implementing and complying with the minimum requirements set forth in this Manual and includes the following six primary activities:

- Submitting a PCII accreditation application
- Appointing and training a PCII Officer and PCII Deputy Officer
- Developing an SOP that includes the implementation of the self-inspection program
- Signing an MOA
- Certifying that contractors are providing homeland security support.

Following the PCII Program Office's receipt of the application, the remaining accreditation requirements can be completed in any order.

10.2.1 PCII Accreditation Application

The PCII accreditation application is the official notification to the PCII Program Office of the entity's intention to become accredited. The accreditation application requests the interested entity, points of contact, entity mailing address, initial identification of a PCII Officer and Deputy, proposed use of PCII, and the anticipated scope of the PCII program within that entity. The application may be submitted electronically or by fax or mail to the addresses and numbers listed at the front of this Manual. The PCII Program Office will contact the accreditation candidate once it has received and reviewed the application. The PCII Program Office reviews the application to determine the entity's eligibility to access PCII under the CII Act and the Regulation, notably the entity's Federal, State, or local government status and its demonstrated need to use PCII as specified in the CII Act and the Regulation. Appendix 11 provides a sample PCII Accreditation Application.

10.2.2 PCII Officer and Deputy PCII Officer

PCII Officer

Each entity is required to nominate an individual as a PCII Officer. A candidate for the PCII Officer position must have the ability to carry out the PCII Officer's roles and responsibilities (see Section 2.1, "PCII Officer Responsibilities") and the authority to allocate resources to comply with the CII Act, the Regulation, this Manual, and other PCII Program Office guidance. In addition to the PCII Officer, each accredited entity must appoint a Deputy PCII Officer who can serve as an alternate as needed and assist the PCII Officer in managing the entity's PCII program. If the PCII Officer or Deputy PCII Officer is not a Federal government employee, he or she must execute an NDA.

The nominated PCII Officer and Deputy PCII Officer must take the PCII Officer training and pass a certification examination following the training. The PCII Officer should contact the PCII Program Office to determine the dates and location of the PCII Officer training. Additional information about PCII Program training requirements can be found in Section 9, "PCII Training Program". Once the candidate has passed the training, the PCII PM will appoint the PCII Officer and Deputy PCII Officer. A sample PCII Officer appointment letter can be found in Appendix 12.

If the PCII Officer or Deputy PCII Officer leaves or needs to be replaced, the entity must notify the PCII Program Office in writing as soon as possible after the departure of the incumbent PCII Officer. The entity should nominate a new PCII Officer or Deputy PCII Officer immediately in coordination with the PCII Program Office and ensure that the new PCII Officer or Deputy PCII Officer receives the required training and certification. Until the new PCII Officer is appointed by the PCII Program Office, the Deputy PCII Officer serves as the PCII Officer.

Assistant PCII Officers

In most cases, the PCII Officer and Deputy PCII Officer cannot undertake their responsibilities alone. Therefore, the entity is encouraged to designate one or more Assistant PCII Officers and include other staff to assist in the implementation and management of the entity's PCII program. An Assistant PCII Officer must at a minimum be trained as a PCII user. If the Assistant PCII

Officer is not a Federal employee, he or she must also sign an NDA. Furthermore, if the Assistant PCII Officer will be fulfilling the various obligations of a PCII Officer, including undertaking roles and responsibilities set forth in Section 2.1, "PCII Officer Responsibilities", the Assistant PCII Officer is subject to the same training requirements as the PCII Officer.

10.3 STANDARD OPERATING PROCEDURES AND THE SELF-INSPECTION PROGRAM

As part of an entity's accreditation process, the PCII Officer must develop SOPs that establish the entity's PCII handling, safeguarding, and dissemination procedures. The PCII Program Office will provide a model SOP that the entity can use to draft its own procedures. The PCII Officer also can customize the SOPs or use the entity's own SOPs provided that he or she implements the PCII Program's baseline handling and safeguarding requirements. The SOPs must include a self-inspection process that the entity must implement in conjunction with the PCII Program Office.

A PCII Program Office-supervised self-inspection program is an integral part of an entity's accreditation process. The self-inspection program consists of two phases: an implementation phase and an oversight and monitoring phase. The self-inspection activities administered by the PCII Program Office and the accredited entity together provide an assessment of the level of activity and compliance with PCII Program regulations and requirements.

The PCII Program Office is responsible for the overall management of the self-inspection program and will work with the PCII Officer to implement the self-inspection process. Section 12, "Oversight and Compliance", provides additional details about the oversight and compliance phase of the self-inspection and the PCII Program Office's role.

The implementation phase of the self-inspection consists of the PCII Officer reviewing PCII Program Office templates relating to the entity's PCII program and developing SOPs. In a second monitoring phase of the self-inspection, the accredited entity is required to complete self-inspection of PCII activity on no less than an annual basis and provide an annual report to the PCII Program Office based on the self-inspection. Section 12.2.2, "Self-Inspection", provides additional details about the monitoring and oversight phase of the self-inspection plan.

10.4 MEMORANDUM OF AGREEMENT

A senior official with the authority to represent the entity, and who can commit the entity to participate in the PCII Program, is required to enter into the MOA with DHS. Separate MOAs for Federal entities and State and local entities can be found in Appendix 14 and Appendix 15. The MOA sets forth the PCII Officer's responsibilities and obligations as well as the requirements for handling, using, disseminating, and safeguarding PCII throughout the Federal, State, or local entity. In addition, the MOA constitutes an entity-wide obligation and an executive-level commitment to achieving and maintaining PCII accreditation.

10.5 CONTRACTOR CERTIFICATION

The Regulation requires that before Federal, State, and local government contractors can access PCII, the PCII PM or PCII Officer must certify that they are performing services in support of the purposes of the CII Act. All contractors must sign NDAs and complete the PCII Authorized

User Training before they can access PCII. These requirements apply to all contractors within a government entity who will access PCII.

The Regulation also requires that contractors accessing PCII agree by contract to comply with PCII Program requirements. As contracting companies accessing PCII are identified, the PCII Program Office, in coordination with the contractors' PCII Officer, will work to incorporate approved PCII-contract language into the contractors' contracts. Appendix 18 provides the PCII contract language.

Although the certification is a pre-requisite to the contractor accessing PCII, the contract modification can be done at a later date but must be accomplished as soon as practicable.

At the time an entity is applying for accreditation, the PCII Officer will initiate the following contractor certification process:

- The PCII Officer must retain a list of all subcomponents of the accredited entity that have homeland security responsibilities, employ contractor support in completing their duties, and use or are planning on using PCII.
- The PCII Officer will evaluate the contractor's support of the entity to ensure that the contractor is performing services in support of the purposes of the CII Act. The PCII Officer must record the name of the contractor entity and confirm in writing that the contractor is performing services in support of the purposes of the CII Act. If, in exigent circumstances or otherwise, all contracting companies cannot be identified or if it would require considerable resources to do so, the PCII Officer should identify the organizations within his or her entity that use the services of contractors in support of homeland security duties. Appendix 17 contains the Contractor Certification Memorandum for the Record that the PCII Officer should use when certifying contractors.
- The PCII Officer must work with the contractors requiring access to PCII to amend their contracts to include language stipulating that the contractor will comply with all relevant requirements of the PCII Program, including the CII Act, the Regulation, and the requirements set forth in this Manual. If all contracting companies cannot be identified or if it would require considerable resources, contractors can modify their contracts after accessing PCII. The contractors, however, must be certified by the PCII Officer before they can access PCII.
- The inclusion of the relevant PCII language set forth in Appendix 18 in applicable contracts may require amending existing contracts or including the PCII language in the contract as part of the original contract negotiation.

11. DESTRUCTION OF PCII

This section addresses the appropriate measures and controls for destroying PCII physical materials and electronic copies to ensure that the information cannot be reconstructed. These procedures are derived from the guidance in the Regulation, Section 29.7, "Safeguarding of Protected Critical Infrastructure Information", and applicable DHS Management Directives. The following materials may be destroyed:

- Original submissions determined not to qualify for protection under the provisions of the CII Act (i.e., rejected CII submissions)
- PCII submissions determined to have been incorrectly validated as PCII
- PCII submissions for which the submitter has requested the PCII markings and protections removed
- Copies of PCII materials
- Work products containing PCII.

The unauthorized destruction of Federal records is punishable under the provisions of the Federal Records Act. In the case of PCII submissions, this applies only to the original submissions and work products containing PCII. The destruction methods described below must also be used when destroying PCII copies. The decision to dispose of PCII must be consistent with the authorities for Federal records disposition that emanate solely from:

- Departmental records disposition schedules approved by the National Archives and Records Administration (NARA)
- General records schedules published by NARA and applicable throughout the government
- The PCII Program Office's Records Disposition Schedule.

11.1 DESTRUCTION OF ORIGINAL PCII MATERIALS

Only the PCII PM may authorize the destruction of original submissions that were subsequently validated as PCII. Once information is validated as PCII, the PCII Program Office must change the status of PCII to that of non-PCII in order to remove its PCII markings and destroy the material. Status changes may take place only under the circumstances described in Section 5.10, "Post-Validation Change in Status".

Upon making an initial determination that a change in status may be warranted, but prior to a final determination, the PCII Program Office will inform the submitter of the initial determination of a change in status. In so doing, the PCII Program Office should ask whether the submitter prefers that the submission be maintained without the protections of the CII Act, returned to the submitter, or destroyed using the methods described in Section 11.4, "Approved Destruction Methods".

Notice of the final change in status of PCII will be provided to all recipients of that PCII, noting the change in the status of the PCII in question.

The PCIIMS documents the following information about the destruction of original PCII submissions:

- The reason for destroying the submission
- When the original PCII was destroyed
- Who destroyed it.

The PCIIMS retains the Identification Number of all destroyed submissions and documents.

11.2 DESTRUCTION OF WORK PRODUCTS CONTAINING PCII

The destruction of PCII work products must follow the guidance in Section 11.4, "Approved Destruction Methods". PCII Officers are encouraged to track the generation and destruction of all work products containing PCII.

11.3 DESTRUCTION OF COPIES OF PCII MATERIALS

The PCII Program Office encourages the destruction of copies of PCII when they are no longer needed. Approval from the PCII PM or Designee is not required for destroying copies of PCII materials, but the approved destruction methods described in Section 11.4, "Approved Destruction Methods", must be used.

11.4 APPROVED DESTRUCTION METHODS

PCII must be destroyed only by authorized means and approved methods and in accordance with the Federal Records Act, DHS regulations, and the PCII Program Office's Records Disposition Schedule. All destruction of PCII physical materials must ensure that the information cannot be retrieved. Table 11-1 lists the means of destruction approved by the PCII Program for various media.

Table 11-1. Approved Destruction Methods

Type of Media	Approved Destruction Methods
Paper	Shred or Burn
Electronic File	Delete and empty recycle bin
Magnetic Media	Degauss or shred
Compact Discs	Shred and grind
Thumb Drives/Memory Sticks	Wipe and erase data
Microfiche: Audio/Video Tapes	Chemical (e.g., acetone bath) or shred
System Backups	Contact the PCII Program Office
Other (e.g., databases or hard drives)	

Digitized PCII stored in the PCIIMS, all backups, and all other archives must be deleted and destroyed according to processes defined in the PCII Program Office's PCIIMS guidance document, which is based on Federal and DHS requirements. All other Federal, State, and local government entities are required to have commensurate processes in place.

12. OVERSIGHT AND COMPLIANCE

This section provides the procedures for overseeing compliance with PCII Program requirements. All individuals granted access to PCII are responsible for safeguarding it while it is in their possession or control. To that end the PCII Program has developed the training program and other access requirements as set forth in Section 8, "Access, Dissemination and Use", and Section 9, "PCII Training Program". In addition, there is an institution-wide obligation on the part of the entity to oversee and monitor its employees who are accessing PCII. The PCII Officer is responsible for the proper implementation of the procedures set forth in this section in his or her respective entity. The PCII Program Office also has a role and works in conjunction with the PCII Officer as discussed below.

The PCII Officer's oversight of the PCII Program in a given entity consists of—

- Monitoring ongoing compliance with PCII Program requirements
- Performing periodic self-inspections
- Fulfilling an annual reporting requirement
- Investigating any alleged or actual misuse or compromise of PCII
- Reporting any misuse or mishandling of PCII.

The guidance set forth in this section also implements the direction in the Regulation, Section 29.9, "Investigation and Reporting of Violation of PCII Procedures".

12.1 ROLES AND RESPONSIBILITIES

PCII Program stakeholders have the following roles and responsibilities with respect to overseeing compliance with PCII Program requirements set forth in the CII Act, the Regulation, this Manual, and other guidance promulgated by the PCII Program Office:

- The PCII Program Office coordinates with PCII Officers to implement the self-inspection and other oversight activities.
- The PCII Program Office monitors PCII Officers' oversight and compliance activities.
- The PCII Program Office conducts on-site visits to confirm compliance with PCII Program requirements.
- PCII Officers implement the self-inspection plan as agreed upon with the PCII Program Office, including the drafting and implementation of SOPs (See Section 10, "Accreditation").
- PCII Officers in coordination with the PCII Program Office conduct self-inspections on no less than an annual basis to monitor authorized users.
- PCII Officers provide annual reports to the PCII Program Office regarding the status of the PCII program within their entity.
- PCII Officers coordinate the initial investigation into the suspected misuse or mishandling of PCII and immediately report any actual or suspected misuse or mishandling of PCII.

12.2 PROCEDURES FOR OVERSIGHT AND COMPLIANCE

A PCII Officer oversees the use of PCII within an accredited entity. All authorized users within the entity are assigned to the PCII Officer who is responsible for implementing and monitoring the appropriate safeguarding of PCII. The PCII Officer supervises the authorized users who are individually accountable for properly handling and safeguarding PCII. If PCII users are not part of an accredited entity, the PCII Program Office is responsible for overseeing such users and ensuring that they comply with all PCII requirements.

Designees are responsible for managing the authorized users accessing PCII submitted under a categorical inclusion overseen by the Designee.

12.2.1 Oversight Activities

There are a number of monitoring and oversight activities that a PCII Officer must undertake, notably—

- Conducting the self-inspection and providing annual reports to the PCII Program Office
- Undertaking site visits
- Conducting system audits.

The self-inspection provides the first level of oversight and on-site visits provide a second level of scrutiny of PCII program activity within an entity. In addition, the PCII Program Office, the PCII Officer, and the Designee must conduct system audits throughout the accreditation life cycle to ensure that the systems conform to PCII Program requirements and are properly safeguarding and tracking PCII.

12.2.2 Self-Inspection

The self-inspection is the PCII Program Office's and PCII Officer's primary monitoring and oversight tool. The self-inspection is conducted primarily through the issuance of questionnaires to authorized users, PCII Officers, and Designees following the anniversary of the later of the PCII Officer training or the signing of the MOA by a government entity. The questionnaires, developed by the PCII Program Office, are specific to each role and serve to provide a picture of use and handling by all authorized users, PCII Officers, and Designees.

The PCII Program Office will provide additional guidance for PCII Officers regarding the issuance of the questionnaires, system audits, and site visits.

There are two broad lines of questioning: one line is directed at authorized users and another is directed at PCII Officers and Designees.

Authorized Users

The PCII Officer sends out 2 different questionnaires in succession to authorized users under his or her purview. Table 12-1 summarizes the purpose of each level of questions, the targeted respondents, and the method for answering the questions. The PCII Officer collaborates with the

PCII Program Office to consolidate and analyze answers from the questionnaires and to determine the next steps in the self-inspection process.

Table 12-1. Authorized User Questionnaires

Authorized User Questionnaires			
Level	**Purpose**	**Respondents**	**Method of Completion**
1	Measure general practices and PCII usage and identify potential risks and non-compliance with safeguarding requirements	All authorized users under the purview of the PCII Officer	Multiple choice questionnaire and open ended queries requiring a written response
2	Based on responses to Level 1 questionnaires, contact certain authorized users to get more details about their information sharing practices that may lead or have led to misuse or mishandling of PCII	As needed during each inspection cycle	Administered in person by the PCII Officer or during a telephone interview using standardized set of questions

PCII Officers and Designees

The PCII Program Office sends a questionnaire to the PCII Officer and Designee, summarized in Table 12-2. Based on the responses to the questionnaire, the PCII Program Office interviews a select group of PCII Officers and Designees either in person or over the phone. In the context of a categorical inclusion, the PCII Officer, instead of the PCII Program Office, may interview the Designee. The PCII Program Office compiles the responses to the PCII Officer and Designee questionnaires.

Table 12-2. PCII Officer and Designee Questionnaires

PCII Officer and Designee Questionnaires			
Level	**Purpose**	**Respondents**	**Method of Completion**
1	Measure general practices and PCII Usage	All PCII Officers and Designees	Multiple choice questionnaire
2	Identify potential risks and non-compliance with safeguarding requirements and investigate practices that may lead or have led to misuse or mishandling of PCII	Select group of PCII Officers and Designees	Administered in person by PCII Program Office staff or during a telephone interview using standardized set of questions

The consolidated responses will enable the PCII Program Office to develop metrics and gauge levels of PCII use and sharing.

12.2.3 Site Visits and System Audits

Site visits by the PCII Program Office or the PCII Officer allow a given site to demonstrate its compliance with the practices and procedures set forth in this Manual and otherwise promulgated by the PCII Program Office. Site assessment teams, whether coordinated by the PCII Program Office or the PCII Officer, are tasked with providing an objective assessment of an entity's ability to meet the requirements set forth in this Manual. Although site visits and system audits are not a requisite oversight activity, they may occur at any time and particularly if the PCII

Program Office or the PCII Officer have identified consistently lax compliance with PCII Program requirements at a given site.

Site Visits and System Audits by the PCII Program Office

The PCII Program Office may elect to conduct a site visit of an accredited entity and any of its subsidiary sites at any time to ensure that the minimum requirements are continually being met or to respond to requests for consultation or guidance from that entity. Should the PCII Program Office choose to visit a site, the Program Office will coordinate with the PCII Officer to find a mutually acceptable time and to ensure that the visit is thorough, efficient, and minimally intrusive.

The PCII Program Office will conduct an ongoing audit of the system repositories of original PCII. Most often the repositories will store categorically included PCII; therefore, the audit of the repository will focus on three areas:

1. The CII being submitted to the repository conforms to the initial information request that the PCII PM validated
2. The repository adequately safeguards and disseminates the original PCII
3. The repository is able to track the dissemination of the original PCII.

If a repository does not store categorically-included PCII but does store other PCII, the audit will consist of steps 2 and 3 listed above.

Site Visits and System Audits by the PCII Officer

PCII Officers may schedule site visits at any time to any location they oversee as part of the accredited entity. The site visit may examine individual use of PCII by authorized users or broad access through a computer-based system. The PCII Officer should coordinate the visit with the on-site personnel who are responsible for overseeing the PCII program on that specific site. Site visits may be part of the regular oversight function carried out by the PCII Officer or may occur in direct response to a suspected or confirmed release.

12.3 VIOLATIONS OF PCII PROCEDURES

In coordination with the DHS Office of Security and the Office of the General Counsel, the PCII PM has established and implemented procedures for reporting and investigating the suspected loss, misplacement, or unauthorized disclosure of PCII. The MOA requires Federal, State, and local entities to cooperate in these investigations. This Section provides further detail about how to proceed in the event of an actual or alleged compromise of PCII.

12.3.1 Investigation of Release of PCII

Persons authorized to access PCII must immediately report any suspected violation of security procedures, the loss or misplacement of PCII, and any suspected and actual unauthorized disclosure of PCII to the PCII PM or the PCII Officer or Designee. An employee appointed by the PCII PM or the Federal, State, or local PCII Officer must conduct a preliminary inquiry for

all reports of actual, alleged, or suspected improper use or disclosure of PCII. This employee must not have been involved in the alleged misuse or disclosure.

The following steps must be taken in the event of an actual, alleged, or suspected release or misuse of PCII:

1. All DHS employees and contractors, participating Federal departments and agencies, and State and local government entities are responsible for immediately reporting to their respective PCII Officers any actual, suspected, or alleged violation of security procedures or loss, misplacement, unauthorized disclosure, or improper use of PCII. When Federal, State, or local government entities' PCII activities are supported by contractors, the contractors are responsible for immediately reporting such actual or suspected violations of PCII policies and procedures to their respective clients. The PCII Officers must immediately inform the PCII Program Office.

    - In the case of entities other than the PCII Program Office, the PCII Officers who receive reports are responsible for reporting the incident to the PCII PM.
    - In the case of the PCII Program Office, the employee's immediate manager is responsible for reporting the incident to the PCII PM.
    - Employees may report a manager's alleged improper use or disclosure of PCII directly to the PCII PM or the DHS Inspector General. Any Federal, State, or local entity accredited to participate in the PCII Program or any individual authorized by those entities to have access to PCII may also report improper use or disclosure of PCII directly to the PCII PM or the DHS Inspector General.

2. The PCII PM—

    - Notifies the DHS Inspector General of the PCII Program's intent to investigate the alleged or actual misuse and mishandling and meets with the DHS Inspector General to the extent necessary
    - Assigns a staff member to lead the investigation and decides whether a PCII Program Office representative must travel to the location of the suspected release
    - Directs the PCII Officer to begin gathering information regarding the release that will enable the drafting of the report cited in number 3 below
    - Assesses any potential damage
    - Takes any immediate action to mitigate damages.

3. The PCII PM, with the assistance of the PCII Officer, initiates the preliminary investigation and prepares a report in the form provided in Appendix 19, PCII Loss or Misuse Report, that establishes, to the extent possible:

    - Identification Number(s) of the PCII
    - Date of the release
    - Responsible party
    - Date that the release was discovered
    - The cause of the release; whether it is considered accidental or intentional; and whether it is actual, suspected, or alleged

- The potential damage resulting from the misuse or disclosure
- Any actions taken to mitigate any damage caused by the disclosure.

4. The PCII PM, in consultation with the DHS OGC, will review the findings and determine if a violation of procedures, loss of information, and/or unauthorized disclosure or use has occurred.

5. If the investigation reveals any evidence of wrongdoing, the DHS Office of General Counsel must contact the Department of Justice's Criminal Division for consideration of prosecution under the criminal penalty provisions of Section 214(f) of the CII Act.

6. If there is evidence of wrongdoing by an employee of a State or local entity or a contractor, the MOA requires the State or local entity to pursue all available options to prosecute the individual who mishandled the PCII. State and local entities are expected to establish and implement policies and processes to take disciplinary action against their employees who do not follow proper procedures for using, safeguarding, and handling PCII. Although applicable sanctions may differ among State and local employees, the viability and integrity of the PCII Program depends on these employees' compliance with the same use and handling requirements set forth in the CII Act, the Regulation, and this Manual. Before they can access PCII, State and local government entities must agree to treat breaches by their employees or contractors as matters subject to the criminal code or to the applicable employee code of conduct for the jurisdiction. If any State or local government PCII user discloses PCII without authorization or uses it inappropriately, the State or local government entity's accreditation will be jeopardized and the entity could lose its access to PCII. Moreover, the State or local PCII user will be subject to the rules of conduct (including sanctions) that apply generally to the State or local entity's employee. Any PCII loss or misuse must also be referred to the appropriate authorities for prosecution under State criminal law.

7. If the investigation and report confirm the release of PCII, the PCII Program Office notifies the submitter that a release has occurred and provides an assessment of the potential impact of the release, unless the notification could reasonably be expected to hamper the relevant investigation or adversely affect any other related national security, homeland security, or law enforcement interests. While the initial notification may be verbal, the PCII PM will send the submitter a written notification.

8. At the direction of the PCII PM, the PCII Officer undertakes any additional corrective action to mitigate any negative impacts.

12.3.2 Disciplinary Actions

In addition to the disciplinary actions mentioned above, and depending on the severity of the violation, the PCII PM can take further action, such as revoking an entity's accreditation status and thus its access to PCII or an entity's authority to receive categorically included PCII.

12.4 SUSPICIOUS OR INAPPROPRIATE REQUESTS

Suspicious or inappropriate requests for PCII by any means (e.g., e-mail or verbal), must be reported immediately:

- **External to the PCII Program Office.** Such requests must be reported to the PCII Officer, who must then report them to the PCII PM.
- **Internal to the PCII Program Office.** Such requests must be reported to the PCII PM.
- **Within DHS.** Upon being informed of such a request, the PCII PM must immediately report it to the DHS Office of Security.

Protected Critical Infrastructure Information Program

Procedures Manual

Appendices

April 2009

Table of Contents

Appendix 1 Abbreviations and Acronyms

ABBREVIATIONS AND ACRONYMS	
ASIP	Assistant Secretary for Infrastructure Protection
ATO	Agreement to Operate
C.F.R.	Code of Federal Regulations
CII	Critical Infrastructure Information
CII Act	Critical Infrastructure Information Act of 2002
DHS	Department of Homeland Security
FFRDC	Federally Funded Research and Development Center
FOIA	Freedom of Information Act
GAO	Government Accountability Office
IG	Inspector General
ISAO	Information Sharing and Analysis Organization
MOA	Memorandum of Agreement
NARA	National Archives and Records Administration
NDA	Non-Disclosure Agreement
PCII	Protected Critical Infrastructure Information
PCIIMS	PCII Management System
PGP	Pretty Good Privacy®
SOP	Standard Operating Procedure
SRD	System Requirements Document
U.S.C.	United States Code
VA	Validation Analyst

Appendix 2 Definitions

Unless otherwise specified, the PCII Program Procedures Manual uses the definitions in Sections 2 and 212 of the *Homeland Security Act* and Section 29.2 of the Regulation.

Accreditation. A program that ensures that Federal (including DHS), State, and local government entities have a clear understanding of, and are monitored in, their handling, use, dissemination and safeguarding of PCII. The PCII accreditation program:

- Prescribes adequate safeguarding measures and minimum requirements,
- Ensures that PCII is handled and disseminated in accordance with the CII Act, the Regulation, and this Manual, and
- Educates and trains PCII users in the proper handling, use, dissemination, and safeguarding of PCII.

Agreement to Operate (ATO). An agreement, executed by the PCII Program Manager (PM) and a senior official within an entity receiving PCII, enumerating the obligations of both the PCII Program Office and the recipient entity with respect to the receipt, validation, safeguarding, and dissemination of submitted critical infrastructure information and validated PCII in the entity's possession. The ATO is program specific within a Federal accredited entity that has a categorical inclusion program, or within a State or local entity that has a PCII repository.

Assistant PCII Officer. An individual, trained as either an authorized user of PCII or as a PCII Officer, who is responsible for the management of the PCII Program at a specific site or for a specific system, and who is accountable to the PCII Officer and the Deputy PCII Officer for that site.

Authorized User. An individual (i.e., a Federal, State, or local government employee or contractor) who has been trained in the appropriate use and dissemination of PCII and has homeland security duties. In addition, all non-Federal government employees must sign a Non-Disclosure Agreement (NDA) to access PCII. Before accessing PCII, an Authorized User must have a need-to-know that PCII.

Categorical Inclusion. A declaration by the PCII Program Manager that information of a certain subject matter or type, when properly submitted, will be considered validated as PCII upon receipt by the PCII Program Office or any of the Designees. Categorical inclusion programs are negotiated prior to the receipt of submissions.

Contractor. Contractors include Federal, State and local contractors. For the purposes of this manual, the term "Federal contractors" includes Federally Funded Research and Development Centers (FFRDC).

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

Critical Infrastructure Information (CII). Information that is not customarily in the public domain and is related to the security of critical infrastructure or protected systems. CII consists of records and information concerning any of the following:

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

Deputy PCII Officer. An individual, nominated by his or her entity and appointed by the PCII PM after the completion of all training requirements. The Deputy PCII Officer must be able to (1) assist the PCII Officer with the management and oversight of the entity's PCII Program and (2) assume all PCII Officer roles and responsibilities in the event the PCII Officer is absent.

Designee. A Federal employee outside 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 PCII PM, on a case by case basis. The PCII Program Manager will appoint a Designee only to manage a categorical inclusion program. The PCII Officer supervises the Designee within a given Federal entity.

Distributed Data Framework. The PCII Program's information sharing framework, wherein PCII resides on multiple systems at the Federal, State and local levels. The PCII management system retains the metadata associated with all original PCII.

Exigent Circumstances. Other than in circumstances set forth in Section 29.8(e) of the Regulation, exigent circumstances encompass all hazards and mean instances in which there is a serious threat of loss of life, physical injury, and/or serious damage to property. Such incidents can be human-caused or natural and require responsive action to protect life and property. In exigent circumstances, certain PCII handling and safeguarding requirements may be suspended.

Freedom of Information Act (FOIA). This law (5 United States Code § 552) establishes a presumption that records in the possession of Executive Branch agencies and departments are available to the public. It is the vehicle under which the public may request Federal Government records in accordance with its requirements. Pursuant to the CII Act, PCII is exempt from disclosure under FOIA. The FOIA exemption applicable to PCII is b(3):

(b) [FOIA] ... does not apply to matters that are:

(3) Specifically exempted from disclosure by statute ... provided such statute
(A) Requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or
(B) Establishes particular criteria for withholding or refers to particular types of matters to be withheld.

Information that is separately exempt from disclosure under FOIA or applicable State or local law does not lose its separate exemption protection due to the applicability of procedures established to implement the CII Act or any failure to follow those procedures.

Guidance Documents. Documentation, including guidelines and formalized standard operating procedures, generated by the PCII Program Office that inform participants in the PCII Program of specific tasks they must undertake to accomplish PCII safeguarding and handling requirements.

In the Public Domain. Information is said to be "in the public domain" when it is 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.

Information Sharing and Analysis Organization (ISAO). Any formal or informal entity or collaboration created or employed by public or private sector organizations for purposes of:

- Gathering and analyzing critical infrastructure information to better understand the security problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability thereof;
- Communicating or disclosing critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or an incapacitation problem related to critical infrastructure or protected systems; and
- Voluntarily disseminating critical infrastructure information to its members, Federal, State and local governments, or any other entities that may be of assistance in carrying out the purposes specified above.

Local Entity or Local Government. Encompasses the following:

- 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
- An Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation

- A rural community, unincorporated town or village, or other public entity.

Memorandum of Agreement (MOA). A written agreement between the PCII Program Office and a non-DHS Federal department or agency, a State government, or a local government with which PCII will be shared that sets forth the responsibilities and minimum requirements for handling, using, and safeguarding PCII. The execution of a MOA is a prerequisite to an entity becoming accredited.

Metadata. Metadata consists of data about data. An item of metadata may describe an individual datum, or content item, or a collection of data including multiple content items and hierarchical levels, for example a database schema. The PCII Program Office has defined a specific set of metadata relating to PCII, that describes the submitter, the CII involved, and the status of the submission. The metadata for all submissions consists of—

- Receipt of submissions
- Contact information of the submitter and Designee
- Validation determinations
- Storage location of original PCII
- Amendments or additions to original PCII submissions

Need-to-know. The determination made by an authorized user of information that a prospective recipient requires access to specific information to perform or assist in a lawful and authorized governmental function, i.e., access is required for the performance of official duties.

Original PCII. CII submitted to the PCII Program Office or Designee and validated as PCII.

Original PCII Repository. Electronic or paper storage of original PCII (not copies of original PCII) maintained by the PCII Program Office or a Designee.

PCII. See Protected Critical Infrastructure Information.

PCII Officer. An employee or contractor of a Federal, State or local government entity, who is nominated by his or her entity and appointed by the PCII PM after the completion of all training requirements. Every accredited entity must have a PCII Officer.

PCII Management System (PCIIMS). A system managed by the PCII Program Office that records information regarding the receipt, acknowledgement, validation, storage, destruction, and dissemination of PCII.

Protected Critical Infrastructure Information (PCII). PCII refers to all critical infrastructure information, including categorical inclusion PCII, that has undergone the validation process and that the PCII Program Office has determined qualifies for protection under the CII Act. All information submitted to the PCII Program Office or Designee with an express statement is presumed to be PCII until the PCII Program Office determines otherwise.

Protected System. The term *protected system:*

- Means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure
- 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.

Protection Statement. Means the statement set forth below that must be included on any PCII.

WARNING

This document contains Protected Critical Infrastructure Information (PCII). In accordance with the provisions the Critical Infrastructure Information Act, 6 U.S.C. §§ 131 *et seq.*, it is exempt from release under the Freedom of Information Act (5 U.S.C. 552) and similar State and local disclosure laws. Unauthorized release may result in criminal and administrative penalties. It is to be safeguarded and disseminated in accordance with the Critical Infrastructure Information Act, 6 U.S.C. §§ 131 *et seq.*, the implementing Regulation, 6 C.F.R. Part 29 and PCII Program requirements.

Regulation. The "Procedures for Handling Critical Infrastructure Information; Final Rule" codified at 6 Code of Federal Regulations Part 29, as amended, implementing the CII Act.

Regulatory Proceedings. Administrative proceedings in which DHS is the adjudicating entity. This does not include any form or type of regulatory proceeding or other matter outside of DHS.

Requested Limited Dissemination. An additional, optional restriction on the destination of a submitter's CII, in which the dissemination of the information is limited to a pre-determined list of potential recipients provided by the submitter. The PCII Program Office will accommodate requested limited dissemination to the extent the request does not conflict or interfere with DHS' mission. Further details are provided in Section 8.2.1 of the PCII Program Procedures Manual.

Self-Inspection. An oversight and reporting program in which the PCII Officer is responsible for reviewing and assessing his or her entity's compliance with PCII Program Office guidance on the handling, use, and storage of PCII. The self-inspection consists of three phases. The first is an implementation phase during which the PCII Officer works with the PCII Program Office to establish a PCII program within the Officer's entity. The second phase is an oversight phase whereby the PCII Officer, with the assistance of the PCII Office, monitors the PCII program within the entity. The final phase consists of periodic reporting by the PCII Officer to the PCII Program Office, including an annual report. More information about the Self-Inspection can be found in Section 12.2.2 of the PCII Program Procedures Manual.

Senior Official. An individual within an entity who has the authority to legally bind that entity to the PCII Program's Memorandum of Agreement and any other requirements of the PCII Program Office, as well as the authority to allocate the personnel and financial resources of that entity.

Submitted in Good Faith. The Regulation states that any information submitted for validation as PCII that could be reasonably defined as CII or PCII is deemed to have been submitted in good faith. Upon validation of a submission as PCII, DHS has conclusively established the good

faith of the submission. Any information qualifying for PCII protections under a categorical inclusion identified by the PM is submitted in good faith.

Voluntary/Voluntarily. A submission is considered voluntary if it is submitted in the absence of DHS' exercise of legal authority to compel access to or submission of such information.

The following information is not considered voluntary and therefore is expressly not eligible for protection under the CII Act:

- 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))—
  - Information or statements contained in any documents or materials filed with the Securities and Exchange Commission, or with Federal banking regulators, pursuant to section 12(i) of the Securities Exchange Act of 1934 (15 U.S.C. § 781(I)); and
  - Any disclosure or writing that when made accompanied the solicitation of an offer or a sale of securities; and
- Information or statements previously submitted to DHS in the course of a regulatory proceeding or a licensing or permitting determination.

The submission of CII 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 will also be considered voluntary submissions.

Appendix 3 Critical Infrastructure Information Act of 2002

The Critical Infrastructure Information Act of 2002 (CII Act) is Title II, Subtitle B of the Homeland Security Act of 2002, Public Law 107-296.

Subtitle B—Critical Infrastructure Information

SEC. 211. SHORT TITLE.
This subtitle may be cited as the "Critical Infrastructure Information Act of 2002**.**"

SEC. 212. DEFINITIONS.
In this subtitle:
(1) AGENCY.—The term "agency" has the meaning given it in section 551 of title 5, United States Code.
(2) COVERED FEDERAL AGENCY.—The term "covered Federal Agency" means the Department of Homeland Security.
(3) CRITICAL INFRASTRUCTURE INFORMATION.—The term "critical infrastructure information" means information not customarily in the public domain and related to the security of critical infrastructure or protected systems—

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

(4) CRITICAL INFRASTRUCTURE PROTECTION PROGRAM.—The term "critical infrastructure protection program" means any component or bureau of a covered Federal Agency that has been designated by the President or any Agency head to receive critical infrastructure information.
(5) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term "Information Sharing and Analysis Organization" means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of—

(A) gathering and analyzing critical infrastructure information 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;
(B) communicating or disclosing critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of a interference, compromise, or a incapacitation problem related to critical infrastructure or protected systems; and

(C) voluntarily disseminating critical infrastructure information to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).

(6) PROTECTED SYSTEM.—The term "protected system"—

(A) 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

(B) 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.

(7) VOLUNTARY.—

(A) IN GENERAL.—The term "voluntary", in the case of any submittal of critical infrastructure information to a covered Federal Agency, means the submittal thereof in the absence of such agency's exercise of legal authority to compel access to or submission of such information and may be accomplished
by a single entity or an Information Sharing and Analysis Organization on behalf of itself or its members.

(B) EXCLUSIONS.—The term "voluntary"—

(i) 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))—

(I) does not include information or statements contained in any documents or materials filed with the Securities and Exchange Commission, or with Federal banking regulators, pursuant to section 12(i) of the Securities Exchange Act of 1934 (15 U.S.C. 781(I)); and

(II) with respect to the submittal of critical infrastructure information, does not include any disclosure or writing that when made accompanied the solicitation of an offer or a sale of securities; and

(ii) does not include information or statements submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings.

SEC. 213. DESIGNATION OF CRITICAL INFRASTRUCTURE PROTECTION PROGRAM.

A critical infrastructure protection program may be designated as such by one of the following:

(1) The President.

(2) The Secretary of Homeland Security.

SEC. 214. PROTECTION OF VOLUNTARILY SHARED CRITICAL INFRASTRUCTURE INFORMATION.

(a) PROTECTION.—

(1) IN GENERAL.—Notwithstanding any other provision of law, critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered Federal Agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an Express Statement specified in paragraph (2)—

(A) shall be exempt from disclosure under section 552 of title 5, United States Code (commonly referred to as the Freedom of Information Act);
(B) shall not be subject to any agency rules or judicial doctrine regarding ex parte communications with a decision making official;
(C) shall not, without the written consent of the person or entity submitting such information, be 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 if such information is submitted in good faith;
(D) shall not, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or employee of the United States for purposes other than the purposes of this subtitle, except—
(i) in furtherance of an investigation or the prosecution of a criminal act; or
(ii) when disclosure of the information would be—
(I) 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
(II) to the Comptroller General, or any authorized representative of the Comptroller General, in the course of the performance of the duties of the General Accounting Office.
(E) shall not, if provided to a State or local government or government agency—
(i) be made available pursuant to any State or local law requiring disclosure of information or records;
(ii) otherwise be disclosed or distributed to any party by said State or local government or government agency without the written consent of the person or entity submitting such information; or
(iii) be used other than for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act; and
(F) does not constitute a waiver of any applicable privilege or protection provided under law, such as trade secret protection.

(2) EXPRESS STATEMENT.—For purposes of paragraph (1), the term "Express Statement", with respect to information or records, means—
(A) in the case of written information or records, a written marking on the information or records substantially similar to the following: "This information is voluntarily submitted to the Federal Government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002."; or
(B) in the case of oral information, a similar written statement submitted within a reasonable period following the oral communication.

(**b) LIMITATION**.—No communication of critical infrastructure information to a covered Federal Agency made pursuant to this subtitle shall be considered to be an action subject to the requirements of the Federal Advisory Committee Act (5 U.S.C. App. 2).
(c) INDEPENDENTLY OBTAINED INFORMATION.—Nothing in this section shall be construed to limit or otherwise affect the ability of a State, local, or Federal government entity,

agency, or authority, or any third party, under applicable law, to obtain critical infrastructure information in a manner not covered by subsection (a),
including any information lawfully and properly disclosed generally or broadly to the public and to use such information in any manner permitted by law.

(d) TREATMENT OF VOLUNTARY SUBMITTAL OF INFORMATION.—
The voluntary submittal to the Government of information or records that are protected from disclosure by this subtitle shall not be construed to constitute compliance with any requirement to submit such information to a Federal Agency under any other provision of law.

(e) PROCEDURES.—

(1) IN GENERAL.—The Secretary of the Department of Homeland Security shall, in consultation with appropriate representatives of the National Security Council and the Office of Science and Technology Policy, establish uniform procedures for the receipt, care, and storage by Federal agencies of critical
infrastructure information that is voluntarily submitted to the Government. The procedures shall be established not later than 90 days after the date of the enactment of this subtitle.

(2) ELEMENTS.—The procedures established under paragraph (1) shall include mechanisms regarding—

(A) the acknowledgement of receipt by Federal agencies of critical infrastructure information that is voluntarily submitted to the Government;

(B) the maintenance of the identification of such information as voluntarily submitted to the Government for purposes of and subject to the provisions of this subtitle;

(C) the care and storage of such information; and

(D) the protection and maintenance of the confidentiality of such information so as to permit the sharing of such information within the Federal Government and with State and local governments, and the issuance of notices and warnings related to the protection of critical infrastructure and protected systems, in such manner as to protect from public disclosure the identity of the submitting person or entity, or information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is otherwise not appropriately in the public domain.

(f) PENALTIES.—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 critical infrastructure information protected from disclosure by this subtitle coming to him in the course of this 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 1 year, or both, and shall be removed from office or employment.

(g) AUTHORITY TO ISSUE WARNINGS.—The Federal Government may provide advisories, alerts, and warnings to relevant companies, targeted sectors, other governmental entities, or the general public regarding potential threats to critical infrastructure as appropriate. In issuing a warning, the Federal Government shall take
appropriate actions to protect from disclosure—

(1) the source of any voluntarily submitted critical infrastructure information that forms the basis for the warning; or

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

(h) AUTHORITY TO DELEGATE.—The President may delegate authority to a critical infrastructure protection program, designated under Section 213, to enter into a voluntary agreement to promote critical infrastructure security, including with any Information Sharing and Analysis Organization, or a plan of action as otherwise defined in section 708 of the Defense Production Act of 1950 (50 U.S.C. App. 2158).

SEC. 215. NO PRIVATE RIGHT OF ACTION.

Nothing in this subtitle may be construed to create a private right of action for enforcement of any provision of this Act.

The regulation implementing this Act (i.e., 6 Code of Federal Regulations (C.F.R.) Part 29, *Procedures for Handling Protected Critical Infrastructure Information),* is provided in Appendix 4.

Appendix 4 Title 6 Code of Federal Regulations Part 29

Federal Register

Friday,
September 1, 2006

Part IV

Department of Homeland Security
6 CFR Part 29 Procedures for Handling Critical Infrastructure Information; Final Rule

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

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) [3] 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

[3] 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)

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.*

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 [4] 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

[4] 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.

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 andboth apply to actions before the date that information is submitted to the PCII 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–

Appendix 5 Express and Certification Template

EXPRESS STATEMENT

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.

CERTIFICATION STATEMENT

To the best of my knowledge, information, and belief, the information being submitted is not customarily in the public domain.

I attest that I am not submitting this information in lieu of complying with a regulatory requirement.

I am authorized to submit this information to be considered for protection under the Critical Infrastructure Information Act of 2002.

Signature _____ Date _____

Please provide the following information:

Submitter

Name:

Title:

Organization or Company Name (if applicable):

Mailing Address: City: State: Zip:

Office Telephone: Alternate Telephone:

E-mail Address:

Alternate Contact Information:

Name:

Title:

Organization or Company Name (if different from submitter):

Mailing Address: City: State: Zip:

Office Telephone: Alternate Telephone:

E-mail Address:

Please be aware that any knowing or willful false representations provided in this submission may constitute a violation of 18 U.S.C. 1001 and are punishable by fine and imprisonment.

Appendix 6 Agreement to Operate

Agreement to Operate between the Protected Critical Infrastructure Information Program Office and [Federal Agency]

This Agreement to Operate between the Protected Critical Infrastructure Information (PCII) Program Office and the [Federal Agency] sets forth the obligations that each office will assume with respect to information submitted under the [Name of Categorical Inclusion] to be validated as PCII. Both offices will carry out these obligations in accordance with (i) the Critical Infrastructure Information Act of 2002,[5] (ii) 6 C.F.R. Part 29 – Procedures for Handling Critical Infrastructure Information; Final Rule,[6] and (iii) the PCII Program's established procedures. If [Federal Agency] is unable to fulfill the safeguarding requirements defined by the PCII Program Office, all PCII will be transferred to the PCII Program Office.

This Agreement allows [Federal Agency] to receive critical infrastructure information (CII) directly from submitters under the circumstances defined in the attached list of "Roles and Responsibilities under the Agreement to Operate." The PCII Program Office has determined that the [Name of Categorical Inclusion] meet the definition of Categorical Inclusion (See 6 C.F.R. part 29.6 (f)) and may be received directly by [Federal Agency]. Confirmation of this Categorical Inclusion determination has previously been issued to [Federal Agency] by the PCII Program Manager. Further, in support of the Categorical Inclusion, [Federal Agency] must nominate a representative to act as a Program Manager Designee. Upon notification by [Federal Agency], the PCII Program Manager will designate this individual, in writing, as a Program Manager Designee. The Program Manager Designee will be responsible for the receipt, marking, and safeguarding of [Name of Categorical Inclusion]. [Federal Agency] personnel will not have validation responsibilities beyond receiving [Name of document to be received as part of the Categorical Inclusion].

Signed:

[PCII Program Manager]	[Federal Official]
Program Manager	[Title]
PCII Program Office	[Component]
Infrastructure Partnerships Division	[Agency or Department]
Date	Date

5 *The Critical Infrastructure Information Act of 2002,* 6 U.S.C. §§131-134.

6 Procedures for Handling Critical Infrastructure Information; Final Rule, 6 C.F.R. Part 29 (2006).

Roles and Responsibilities under the Agreement to Operate

The Protected Critical Infrastructure Information Program Office shall:

1. Provide copies of all PCII statutes, rules, regulations and other applicable guidance to the designee.
2. Provide access to authorized training and education for all individuals that may access [Name of Categorical Inclusion] designated as PCII.
3. Provide system requirements for the electronic storage and dissemination of PCII.
4. Assist entities seeking access to [Name of Categorical Inclusion] with user authorization and program accreditation.
5. Have the primary responsibility for responding to any requests to publicly disclose any protected [Name of Categorical Inclusion].
6. Provide guidance and assistance with program implementation.

The [Federal Agency Component] **shall**:

1. Appoint a PCII Officer that will provide oversight to PCII use within [Federal Agency]. This person will also serve as the primary liaison between [Federal Agency] and the PCII Program Office. The designee and PCII Officer shall normally be two different people. [Federal Agency] may request that one person serve both roles, but the PCII Program Manager will make the final decision.
2. Conduct routine sampling of submitted [Name of Categorical Inclusion] to verify that supplied information correlates to the question or data request and meets the definition of PCII.
3. Develop procedures to safeguard original PCII that are no less stringent than the requirements defined in the PCII Program Procedures Manual.
4. For DHS and non-DHS individuals who seek access to [Name of Categorical Inclusion], refer them to the PCII Program Office or its training email: pcii-training@dhs.gov to initiate the user authorization process.
5. For any contractor providing services to [Federal Agency Component], provide evidence that the PCII Officer has certified that this person is performing services in support of the purposes of the CII Act. The [Federal Agency] must take action to modify any contract to include special conditions specific to the PCII Program. Contract modification is not a prerequisite for access.
6. Undertake any activities required to properly receive, safeguard, and disseminate PCII, including:
   a. Directly receiving [Name of Categorical Inclusion] defined as critical infrastructure information from submitters;
   b. Properly marking [Name of Categorical Inclusion] according to PCII Program requirements;

c. Assigning a tracking number to each [Name of Categorical Inclusion] received;

d. Securely storing PCII in a manner that prevents unauthorized access and is consistent with PCII Program Office policies;

e. Providing metadata, as defined by the PCII Program Office, for inclusion in the PCII management system;

f. Tracking the dissemination of PCII made from the original submission; and

g. Responding to any request for additional information needed from the submitter.

7. Notify the PCII Program Manager of any procedural changes for the receipt and dissemination of [Name of Categorical Inclusion].

8. Implement and comply with all system requirements, as identified in the PCII Systems Requirement document and subsequent updates.

9. Provide documentation confirming that any information technology system holding PCII has an Authority to Operate from the DHS Chief Information Officer.

10. Coordinate with the PCII Program Office any software modifications that affect the original system requirements.

Appendix 7 Request for Removal of Protections

I, _____ , being an authorized representative of _____ (the "submitter"), request that the Protected Critical Infrastructure Information (PCII) Program Manager change the status of the submitted information bearing the PCII Tracking Number _____ (the "submission") from PCII to non-PCII and that all markings identifying the submission or any of the information contained within the submission as PCII be removed, as provided under section 29.6(g) of the regulation at 6 C.F.R., Part 29, *Procedures for Handling Protected Critical Infrastructure Information*.

I request that all parties who received a copy of the submission or any information contained within the submission be informed of the change in the information's status from PCII to non-PCII.

The requesting party should check one of the following:

☐ I further request that the submission be returned to me, in its entirety, at the address listed below.

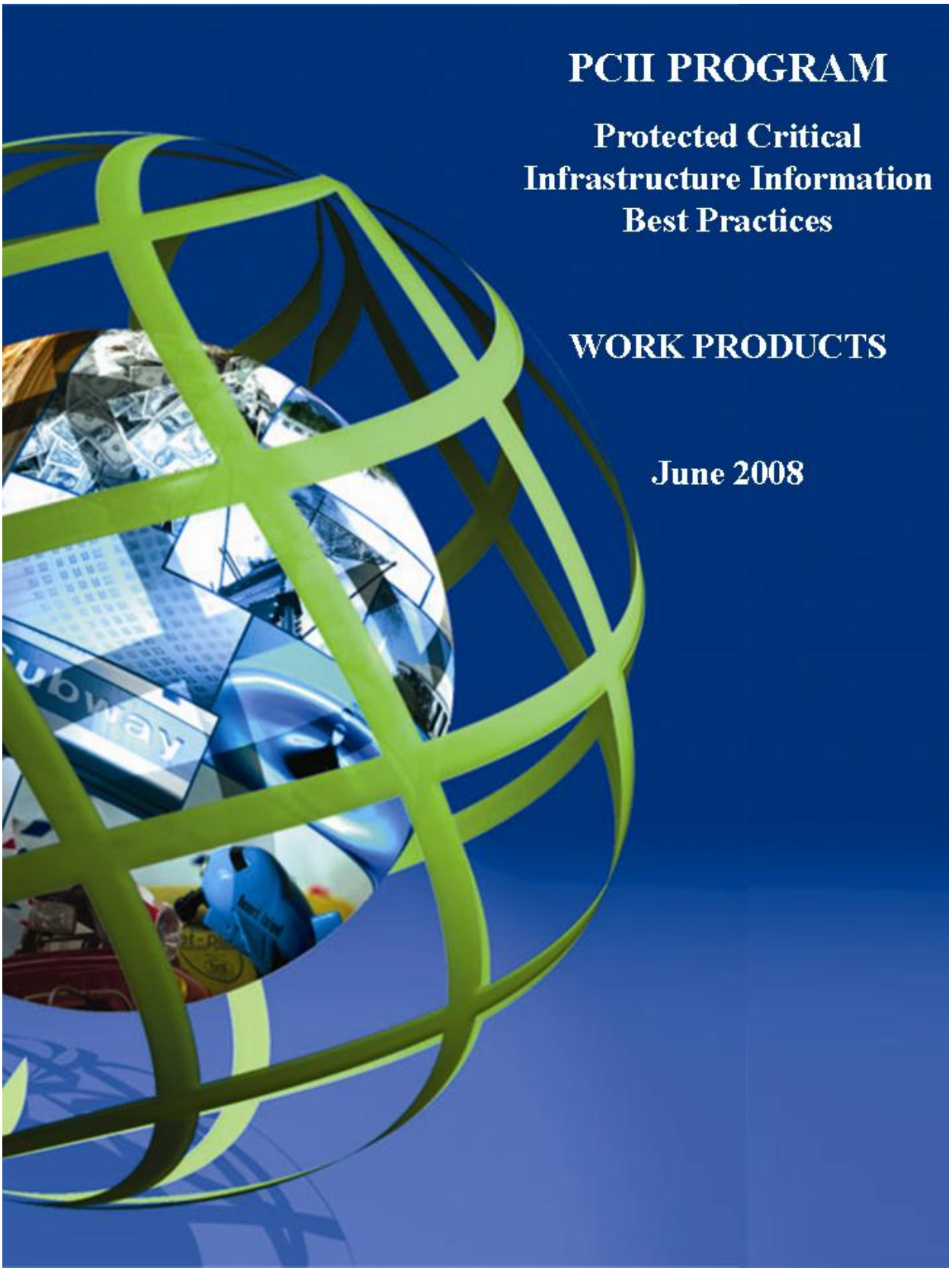
☐ I further request that the submission be destroyed by a method that prevents retrieval of any of the information contained within the submission.

By: _____

Name:
Title:
Date:
Address:

Phone:

Appendix 8 Work Products Guide



GUIDE FOR PCII WORK PRODUCTS:

Marking, Handling, Safeguarding, and Destroying Protected Critical Infrastructure Information (PCII) Work Products

CONTENTS

INTRODUCTION

A user of Protected Critical Infrastructure Information (PCII) occasionally may need to create products that contain or are based upon protected information. These products are subject to special handling and marking procedures.

Remember, if ***any*** PCII is contained in a product, that work product becomes PCII and may not be publicly disclosed. Any information that identifies the submitter of the PCII is also PCII. Such information identifying the submitter may be either explicit (e.g., name of company or individual, or any contact information) or implicit (e.g., name of a product or service, or geographic location). Where a work product contains PCII material (e.g., verbatim PCII, the submitter's identity, or any other proprietary, business sensitive, or trade secret information), that product is PCII and must be handled as PCII.

CATEGORIES OF PCII WORK PRODUCTS

The two primary categories of PCII work products are:

1. Sanitized advisories, alerts, and warnings; and
2. Derivative products: unclassified or classified products derived from and containing PCII

1. SANITIZED PRODUCTS

When Federal, State, or local entities use PCII to prepare advisories, alerts, and warnings and other products regarding potential threats and vulnerabilities to critical infrastructure for dissemination to the public and private sectors or foreign governments, the entity producing such a product must sanitize it. For the purposes of the PCII Program, "sanitization" means distilling the information such that it is not traceable to the submitter and that it does not reveal any information that:

- *Is proprietary, business-sensitive, or trade secret;*
- *Relates specifically to the submitting person or entity (explicitly or implicitly); or*
- *Is otherwise not customarily in the public domain.*

When appropriate and necessary, it is recommended that the PCII Officer contact the submitting person (or an authorized person on behalf of a submitting entity) to ensure that the product does not contain proprietary, business sensitive, or trade secret information. PCII Officers are responsible for ensuring that advisories, alerts, and warnings have been sufficiently sanitized.

When a PCII derivative product is used as the basis for developing an advisory, alert, or warning for public release, paying attention to portion-marking in the derivative product allows the user to ensure that the subsequent advisory, alert, or warning **does not** contain any PCII.

If the PCII derivative product that provides the basis for the advisory, alert, or warning includes "third party information" (e.g., Company A submits information about a product made by, or a service provided by, Company B), the advisory, alert, or warning must **NOT** include anything that explicitly or implicitly identifies EITHER Company or its product or services.

However, as with classified information, analysts may use any information they can derive from open non-PCII sources, even if it is the same information that is also in the PCII derivative product.

Unless exigent circumstances require otherwise, any warning to the general public that is not sanitized in accordance with the directions above must be authorized by the DHS Secretary, the Under Secretary for National Protection and Programs, Assistant Secretary for Cyber Security and Communications, or Assistant Secretary for Infrastructure Protection (ASIP).

Such exigent circumstances exist only when approval of the DHS Secretary, the Under Secretary for National Protection and Programs, Assistant Secretary for Cyber Security and Communications, or the ASIP cannot be obtained within a reasonable time necessary to issue an effective advisory, alert, or warning. The Designee or the PCII Officer must coordinate with the PCII Program Office to issue these warnings in accordance with the Regulation. In issuing advisories, alerts, and warnings, DHS must—

- 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
- 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, any persons or entities on whose behalf the CII was submitted; or is not otherwise appropriately in the public domain.

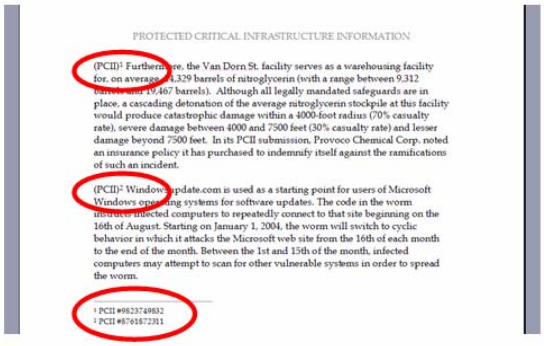
DHS may consult or cooperate with the submitter in making such advisories, alerts, or warnings. A State or local entity that has submitted CII that has been validated as PCII, is not bound to consult DHS in the issuance of an alert, advisory or warning based on such PCII, provided that the State or local entity (a) uses its own copy of the information that has not been marked as PCII or (b) has sanitized the warning such that it does not contain any PCII.

2. DERIVATIVE PRODUCTS

Unclassified Products Derived from and Containing PCII

All users must follow these guidelines when preparing an *unclassified* PCII derivative product:

- Insert the text "Protected Critical Infrastructure Information" in the header and footer in a font larger than the document text.
- Mark each paragraph, table, graphic, figure, etc., containing verbatim or paraphrased PCII parenthetically as "PCII". (All other paragraphs, tables, graphics, figures, etc. are **not** portion-marked.)
- Include the Submission Identification Number for the PCII in a footnote to the paragraph, table, figure, etc. (In most word processing applications this will automatically generate the required reference at the bottom of the page.)


PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

(PCII)[1] Furthermore, the Van Dorn St. facility serves as a warehousing facility for, on average, 14,329 barrels of nitroglycerin (with a range between 9,312 barrels and 19,467 barrels). Although all legally mandated safeguards are in place, a cascading detonation of the average nitroglycerin stockpile at this facility would produce catastrophic damage within a 4000-foot radius (70% casualty rate), severe damage between 4000 and 7500 feet (30% casualty rate) and lesser damage beyond 7500 feet. In its PCII submission, Provoco Chemical Corp. noted an insurance policy it has purchased to indemnify itself against the ramifications of such an incident.

(PCII)[2] Windowsupdate.com is used as a starting point for users of Microsoft Windows operating systems for software updates. The code in the worm instructs infected computers to repeatedly connect to that site beginning on the 16th of August. Starting on January 1, 2004, the worm will switch to cyclic behavior in which it attacks the Microsoft web site from the 16th of each month to the end of the month. Between the 1st and 15th of the month, infected computers may attempt to scan for other vulnerable systems in order to spread the worm.

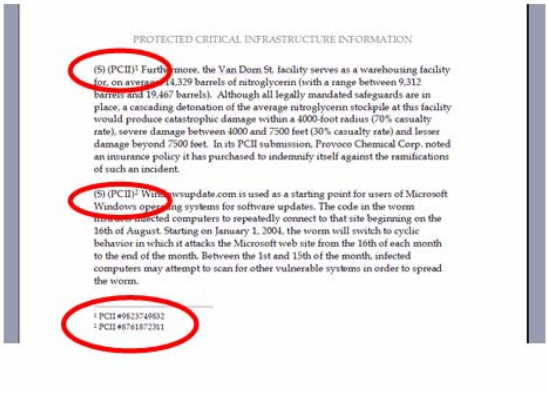
[1] PCII #9823749832
[2] PCII #8761872311

- Affix a PCII Cover Sheet to the derivative product.

Classified Products Derived from and Containing PCII

Classified PCII derivative products must be handled and protected in accordance with the safeguarding and handling requirements for **both** PCII and the highest level of classified designation within the product**.**

All users must follow these guidelines when preparing a *classified* PCII derivative product in addition to the procedures required by the classified designation:


PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

(S) (PCII)[1] Furthermore, the Van Dorn St. facility serves as a warehousing facility for, on average, 14,329 barrels of nitroglycerin (with a range between 9,312 barrels and 19,467 barrels). Although all legally mandated safeguards are in place, a cascading detonation of the average nitroglycerin stockpile at this facility would produce catastrophic damage within a 4000-foot radius (70% casualty rate), severe damage between 4000 and 7500 feet (30% casualty rate) and lesser damage beyond 7500 feet. In its PCII submission, Provoco Chemical Corp. noted an insurance policy it has purchased to indemnify itself against the ramifications of such an incident.

(S) (PCII)[2] Windowsupdate.com is used as a starting point for users of Microsoft Windows operating systems for software updates. The code in the worm [illegible] infected computers to repeatedly connect to that site beginning on the 16th of August. Starting on January 1, 2004, the worm will switch to cyclic behavior in which it attacks the Microsoft web site from the 16th of each month to the end of the month. Between the 1st and 15th of the month, infected computers may attempt to scan for other vulnerable systems in order to spread the worm.

[1] PCII #9623749832
[2] PCII #8761872301

- Insert the text "Protected Critical Infrastructure Information" in the header and footer in a font larger than the document text.
- Each paragraph, table, graphic, figure, etc., containing verbatim or paraphrased PCII must be parenthetically marked as "PCII". (All other paragraphs, tables, graphics, figures, etc. are **not** portion-marked.) Where information in a paragraph, table, graphic, figure, etc., is both PCII and Classified, it must be double-marked [e.g., (S)(PCII) or (TS)(PCII)]. This double marking is necessary because subsequent declassification will eliminate only the requirement for protecting the data as classified information. It will **NOT** eliminate the requirements for protecting PCII.
- Include the Submission Identification Number for the PCII in a footnote to the paragraph, table, figure, etc. (In most word processing applications this will automatically generate the required reference at the bottom of the page.)
- Affix a PCII Cover Sheet to the derivative product. The PCII Cover Sheet is placed immediately behind the classified Cover Sheet.

The PCII Cover Sheet

The PCII Cover Sheet is a shield that alerts observers that the document contains PCII.

The PCII Cover Sheet must be affixed to all documents containing PCII, including derivative products, and must remain with the document permanently. PCII materials should always be protected by the PCII Cover Sheet, whether in storage, transit, or on a desk, even if that desk is in an environment where the most rigorous access controls are in place.


PROTECTED CRITICAL INFRASTRUCTURE INFORMATION
Requirements for Use

Nondisclosure

By reviewing this cover sheet and accepting the attached PCII you are agreeing not to disclose it to other individuals without following the access requirements and to abide by the guidance contained herein. Your acceptance provides immediate access only to the attached PCII.

Access

Handling

Derivative Products

Submission Identification Number:

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

DISSEMINATION OF DERIVATIVE PRODUCTS

Derivative products can only be disseminated to authorized users with homeland security responsibilities and a "need-to-know". If you need to disseminate a product to unauthorized users or the general public, you are responsible for adequately sanitizing the product and issuing it in the form of an alert, warning, or advisory.

DESTRUCTION OF DERIVATIVE PRODUCTS

The PCII Program Office encourages destruction of PCII derivative products and copies of PCII when no longer needed. No approval is required from the PCII Program Manager for destroying copies of PCII materials or PCII derivative products, but approved destruction methods must be used. Destruction of *original* PCII materials requires approval from the PCII Program Manager. Destruction of these documents must be in accordance with the Federal Records Act or any equivalent State or local records requirements.

Table 8-1. Approved Destruction Methods

Approved Destruction Methods	
Paper	Shred or Burn
Electronic File	Delete and empty recycle bin
Magnetic Media	Degauss or shred
Compact Discs	Shred and grind
Thumb Drives/Memory Sticks	Wipe and erase data
Microfiche: Audio/Video Tapes	Chemical (e.g., acetone bath) or shred
System Backups	Contact the PCII Program Office
Other (e.g., databases or hard drives)	

PCII TRACKING REQUIREMENTS

Users should contact their PCII Officer for instructions on tracking procedures.

Appendix 9 PCII Cover Sheet

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION
Requirements for Use

Nondisclosure

This document contains Protected Critical Infrastructure Information (PCII). In accordance with the provisions of the Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 131 et seq. (the "CII Act"), PCII is exempt from release under the Freedom of Information Act (5 U.S.C. 552) and similar State and local disclosure laws. Unauthorized release may result in criminal and administrative penalties. It is to be safeguarded and disseminated in accordance with the CII Act, the implementing Regulation at 6 C.F.R. Part 29 (the "Regulation") and PCII Program requirements.

By reviewing this cover sheet and accepting the attached PCII you are agreeing not to disclose it to other individuals without following the access requirements and to abide by the guidance contained herein. Your acceptance provides immediate access only to the attached PCII.

If you have not completed PCII user training, you are required to send a request to pcii-training@dhs.gov within 30 days of receipt of this information. You will receive an email containing the PCII user training. Follow the instructions included in the email.

Access

Individuals eligible to access the attached PCII must be Federal, State or local government employees or contractors and must meet the following requirements:

- Assigned to homeland security duties related to this critical infrastructure; and
- Demonstrate a valid need-to-know.

The recipient must comply with the requirements stated in the CII Act and the Regulation.

Handling

Storage: When not in your possession, store in a secure environment such as in a locked desk drawer or locked container. **Do not leave this document unattended**.

Transmission: You may transmit PCII by the following means to an eligible individual who meets the access requirements listed above. In all cases, the recipient must accept the terms of the Non-Disclosure Agreement before being given access to PCII.

Hand Delivery: Authorized individuals may hand carry material as long as access to the material is controlled while in transit.

Email: Encryption should be used. However, when this is impractical or unavailable you may transmit PCII over regular email channels. If encryption is not available, send PCII as a password protected attachment and provide the password under separate cover. **Do not send PCII to personal, non-employment related email accounts.** Whenever the recipient forwards or disseminates PCII via email, place that information in an attachment**.**

Mail: USPS First Class mail or commercial equivalent. Place in an opaque envelope or container, sufficiently sealed to prevent inadvertent opening and to show evidence of tampering, and then placed in a second envelope that has no marking on it to identify the contents as PCII. Envelope or container must bear the complete name and address of the sender and addressee. Envelope will have no outer markings that indicate the contents are PCII and must bear the following below the return address: "**POSTMASTER: DO NOT FORWARD. RETURN TO SENDER**." Adhere to the aforementioned requirements for interoffice mail.

Fax: You are encouraged, but not required, to use a secure fax. When sending via non-secure fax, coordinate with the recipient to ensure that the faxed materials will not be left unattended or subjected to unauthorized disclosure on the receiving end.

Telephone: You are encouraged to use a Secure Telephone Unit/Equipment. Use cellular phones only in exigent circumstances.

Reproduction: Ensure that a copy of this sheet is the first page of all reproductions containing PCII. Clear copy machine malfunctions and ensure all paper paths are checked for PCII. Destroy all unusable pages immediately.

Destruction: Destroy (i.e., shred or burn) this document when no longer needed. For laptops or CPUs, delete file and empty recycle bin.

Sanitized Products	You may use PCII to create a work product. The product must not reveal any information that: • Is proprietary, business sensitive, or trade secret; • Relates specifically to, or identifies the submitting person or entity (explicitly or implicitly); and • Is otherwise not appropriately in the public domain.
Derivative Products	Mark any newly created document containing PCII with "Protected Critical Infrastructure Information" on the top and bottom of each page that contains PCII. Mark "(PCII)" beside each paragraph containing PCII. Place a copy of this page over all newly created documents containing PCII. The PCII Submission Identification Number(s) of the source document(s) must be included on the derivatively created document in the form of a footnote. **For more information about derivative products, see the PCII Work Products Guide or speak with your PCII Officer.**
Submission Identification Number:	

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

Appendix 10 [Intentionally Left Blank]

Appendix 11 PCII Accreditation Application

PCII PROGRAM ACCREDITATION APPLICATION

SUBMIT TO THE PCII PROGRAM OFFICE WHEN COMPLETE

Fax (703) 235-3050

E-mail pcii-accreditation@dhs.gov

As a means to ensure the proper handling and safeguarding of PCII, the Department of Homeland Security (DHS) requests that government organizations interested in using PCII become accredited. This application is the first part of the accreditation process and provides the government entity the opportunity to identify program contacts and proposed PCII usage.

The information requested in this application should document the accreditation entity's proposed PCII program. The PCII Program Office understands that the program structure and/or information requirements may change or evolve as a result of the accreditation entity's operational experience.

GOVERNMENT ENTITY INFORMATION

Date of application (MM/DD/YYYY):

Identify the level of government being accredited:

Name of entity seeking accreditation:

Name of entity responsible for PCII program:

MAILING ADDRESS:
Street or Post Office Box:
City: **State:** **ZIP:**

PHYSICAL ADDRESS: ☐ **Same as above**
Street:
City: **State:** **ZIP:**

TELEPHONE: **FAX:**

E-MAIL ADDRESS: **WEBSITE ADDRESS:**

Mission of entity seeking accreditation:

Estimated number of employees who will use PCII:

Describe the initial plan for sharing PCII within the accredited entity:

Identify the government entities (agencies) initially covered by the accreditation:

Identify future entities (agencies) that may be included under this accreditation:

Identify or describe any planned or ongoing information sharing activities may benefit from using PCII:

Describe the background screening procedures used within the entity seeking accreditation:

Please provide contact information for the entity's disclosure officer:

SENIOR PROGRAM OFFICIAL – CONTACT INFORMATION

NAME:

TITLE:

MAILING ADDRESS ☐ **Same as program information provided above**

Street:

City: **State:** **ZIP:**

TELEPHONE: **FAX:**

E-MAIL ADDRESS:

NOMINATED PCII OFFICER – CONTACT INFORMATION

NAME OF PCII OFFICER:

TITLE:

MAILING ADDRESS ☐ **Same as above**

STREET OR POST OFFICE BOX:

CITY: **STATE:** **ZIP:**

TELEPHONE: **FAX:**

E-MAIL ADDRESS:

Is this person a contractor? ☐ **YES** ☐ **NO**

NOMINATED DEPUTY PCII OFFICER – CONTACT INFORMATION

NAME OF DEPUTY PCII OFFICER:

TITLE:

MAILING ADDRESS ☐ **Same as above**

STREET OR POST OFFICE BOX:

CITY: **STATE:** **ZIP:**

TELEPHONE: **FAX:**

E-MAIL ADDRESS:

Is this person a contractor? ☐ **YES** ☐ **NO**

ASSISTANT PCII OFFICERS – CONTACT INFORMATION (IF APPLICABLE)

NAME OF ASSISTANT PCII OFFICER:

TITLE:

MAILING ADDRESS ☐ **Same as above**

STREET OR POST OFFICE BOX:

CITY: **STATE:** **ZIP:**

TELEPHONE: **FAX:**

E-MAIL ADDRESS:

Is this person a contractor? ☐ **YES** ☐ **NO**

NAME OF ASSISTANT PCII OFFICER:

TITLE:

MAILING ADDRESS ☐ **Same as above**

STREET OR POST OFFICE BOX:

CITY: **STATE:** **ZIP:**

TELEPHONE: **FAX:**

E-MAIL ADDRESS:

Is this person a contractor? ☐ **YES** ☐ **NO**

ADDITIONAL NOMINATED DEPUTY OR ASSISTANT PCII OFFICERS – CONTACT

NAME:

PCII Officer Deputy: ☐

PCII Officer Assistant: ☐

TITLE:

MAILING ADDRESS ☐ **Same as above**

STREET OR POST OFFICE BOX:

CITY: **STATE:** **ZIP:**

TELEPHONE: **FAX:**

E-MAIL ADDRESS:

Is this person a contractor? ☐ **YES** ☐ **NO**

NAME:

PCII Officer Deputy: ☐

PCII Officer Assistant: ☐

TITLE:

MAILING ADDRESS ☐ **Same as above**

STREET OR POST OFFICE BOX:

CITY: **STATE:** **ZIP:**

TELEPHONE: **FAX:**

E-MAIL ADDRESS:

Is this person a contractor? ☐ YES ☐ NO

Appendix 12 PCII Officer Appointment Letter

[Date (Month DD, YYYY)]

MEMORANDUM FOR: [Name of PCII Officer appointee]
[Organization of PCII Officer appointee]
[Address]
[Address]

FROM: Laura L.S. Kimberly, PCII Program Manager

SUBJECT: Appointment of Protected Critical Infrastructure Information (PCII) Officer

Effective immediately and until further notice, [name of PCII Officer appointee] has been appointed as the Protected Critical Infrastructure Information (PCII) Officer for the [organization of PCII Officer appointee].

The PCII Officer is a position established by 6 C.F.R. 29, *Procedures for Handling Critical Infrastructure Information; Interim Rule* (the "Regulation") that implements the Critical Infrastructure Information Act of 2002 (the "CII Act"). The Regulation requires entities that handle PCII, including components of the Department of Homeland Security, to designate a PCII Officer who is the individual within a participating organization responsible for implementing and establishing a program that fulfills all CII Act requirements for PCII. Section 29.4(c) of the Regulation requires that a person appointed to this position "shall be fully familiar with" the PCII procedures established by the PCII Program Manager, and Section 29.4(d) provides that the PCII Officer shall have responsibilities that include procedure implementation, program oversight, and general communication and coordination duties. Some duties of the [organization of PCII Officer appointee]'s PCII Officer are unique to [organization of PCII Officer appointee] and are in addition to general guidance. A Memorandum of Agreement to be entered into by the [organization of PCII Officer appointee] and the PCII Program Office provides further details. The newly designated PCII Officer should become familiar with that agreement. Attached is a list setting forth the responsibilities of the PCII Officer for [organization of PCII Officer appointee]. In addition, this letter serves as notice that [name of PCII Officer appointee] has completed the PCII Training Program and passed the PCII Officer Certification Exam.

In addition to those duties in the attachment, [name of PCII Officer appointee] must keep the PCII Program Office informed of all PCII matters that concern [organization of PCII Officer appointee]. If the PCII Officer has any questions about his or her responsibilities or duties, he or she should contact the PCII Program Office for guidance.

PCII OFFICER ROLES AND RESPONSIBILITIES

ORGANIZATIONAL NEED AND FUNCTION

The PCII regulation at 6 Code of Federal Regulations (C.F.R.) Part 29 implementing the *Critical Infrastructure Information Act of 2002* (CII Act) establish the position and responsibilities of the PCII Officer. The Regulation requires entities that will handle PCII, including components of the Department of Homeland Security (DHS), to designate at least one PCII Officer. Section 29.4(c) of the Regulation requires that a person appointed to this position "shall be fully familiar with" the procedures established by the PCII Program Manager. Section 29.4(d) provides that the PCII Officers shall have responsibilities that include procedure implementation, program oversight, and general communication and coordination duties.

The PCII Officer is the individual within a participating entity responsible for establishing and managing a program that fulfills all requirements for protecting information according to regulations implementing the CII Act and for ensuring the implementation of procedures in accordance with all guidance from the PCII Program Manager. In addition to designating a PCII Officer, each entity must also designate a Deputy PCII Officer to serve as an alternate as needed and to assist in managing the entity's program. The Deputy PCII Officer must meet the same requirements and be able to fulfill all the duties of the PCII Officer. In order to ensure compliance, the PCII Officer must adopt, establish, and implement appropriate policies, procedures, and oversight measures. The PCII Officer, with the assistance of the Deputy and Assistant PCII Officers, is also responsible for ensuring that the entity and each of the associated sites complies with the PCII Accreditation Program minimum requirements and achieves full accreditation in a timely manner. The PCII Program Procedures Manual provides further detailed guidance on the duties of a PCII Officer. The sections on safeguarding, dissemination and use, destruction of PCII, and oversight and compliance are especially relevant.

MAJOR RESPONSIBILITIES OF THE PCII OFFICER AND DEPUTY PCII OFFICER

The major responsibilities of the PCII Officer and the Deputy PCII Officer fall into two categories:

- Procedure implementation, oversight, and compliance; and
- Communication, outreach, and training.

The details are provided in the following table.

	PCII Officer's and Deputy PCII Officer's Roles and Responsibilities
1	Demonstrate full familiarity with the minimum requirements for protecting information according to the CII Act, the Regulation, and the procedures established by the PCII PM.
2	Implement requirements set forth in the MOA.
3	Certify, as appropriate, or assist the PCII PM in certifying, contractors requiring access to PCII, including confirming that their contracts contain appropriate language requiring compliance with PCII Program Office guidance.
4	Ensure the secure sharing of PCII with appropriate authorities and individuals, including: Responding to or assisting with need-to-know inquiries Assisting the PCII Program Office in delivering initial and ongoing training Assisting the PCII Program Office in having the nondisclosure agreements executed and implemented.
5	Designate Assistant PCII Officers as necessary to assist in program implementation.
6	Implement operational procedures, pursuant to guidance given by the PCII Program Office, to ensure that PCII and work products, including derivative materials, alerts, warnings, and advisories, are used, handled, and disseminated appropriately and safeguarded properly. The Guide for PCII Work Products, provides more information.
7	Establish and maintain an ongoing self-inspection program, including periodic review and assessment of the handling, use, and storage of PCII.
8	Coordinate the preliminary investigation into any suspected or actual misuse or loss of PCII. Immediately report any suspected or actual misuse, loss, or unauthorized dissemination of PCII or any suspicious or inappropriate request for PCII to the PCII PM.
9	Ensure that their respective Disclosure Officers are aware that PCII is a Federal record so that the Disclosure Officers are prepared to make an appropriate response to requests for PCII under their respective disclosure laws. The State or local Disclosure Officers must inform requesters that PCII is a Federal record, and that the CII Act protects it from disclosure under all disclosure laws. If the requester has any further questions about the applicability of disclosure laws to PCII, State and local participating entities are encouraged to refer the requester directly to the PCII Program Office or the National Protection and Programs Directorate Disclosure Office.
10	Ensure that the entity's oversight and compliance activities follow PCII Program Office guidance. Develop and implement a process by which the Designee and the entity's PCII Officer will be immediately informed of any suspected violation of PCII security procedures, the loss or misplacement of PCII, or any suspected unauthorized disclosure of PCII within the Designee's entity or entities.
11	Coordinate promptly and appropriately with the PCII PM regarding any request, challenge, or complaint arising from the implementation of the Regulation at 6 C.F.R. Part 29.
12	Participate in meetings with the PCII Program Office, PCII Officer working groups, and other coordination activities regarding PCII, as appropriate.
13	Initiate, facilitate, and promote activities to foster and maintain awareness of PCII policies and procedures.
14	If approached by a potential submitter, act as a PCII advocate to the private sector by providing guidance on appropriate points of contact and courses of action.
15	Participate regularly in PCII training sessions to maintain awareness of program developments.
16	To the extent practicable, remind individuals of their post-employment or PCII program responsibilities.

COMMUNICATION, OUTREACH, AND TRAINING
Coordinate with the PCII Program Manager regarding any request, appeal, challenge, complaint, or suggestion arising out of the implementation of the PCII program within the respective entity.
Participate in meetings with the PCII PO, PCII Officer working groups, and other coordination activities regarding PCII, as appropriate.
Initiate, facilitate, and promote activities to foster and maintain awareness of PCII policies and procedures within the respective entity and at each of the associated sites.
If approached by a potential submitter, act as a PCII advocate to the private sector, by providing guidance on appropriate points of contact and courses of action.
Ensure delivery of initial PCII training and annual refresher training for all program participants within the entity; and maintain records of those individuals who have completed training at each of the entity's associated sites.
Participate regularly in PCII training sessions, including at least one classroom session per year, to maintain awareness of program developments and facilitate annual re-certification.
Ensure that the entity includes a review of post-employment responsibilities to protect PCII as part of its normal out-processing procedures when a PCII user ends his or her participation in the PCII program.

Appendix 13 Congressional Acknowledgement

Acknowledgement of Roles & Responsibilities

Protected Critical Infrastructure Information Program Office

1. Purpose: The purpose of this Acknowledgement of Roles & Responsibilities (Acknowledgement) is to set forth the protocols under which the Department of Homeland Security (DHS) shares Protected Critical Infrastructure Information (PCII) with Congress when requested, and to outline the roles and responsibilities of both DHS and Congressional Authorized Users with regard to the handling of PCII.

2. Background: The Critical Infrastructure Information Act of 2002[1] (CII Act), allows for the disclosure of PCII 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."[2] The implementing Regulation[3] (the Regulation) reiterates the PCII Program's obligation to share PCII with Congress at Congress' request.[4]

   The CII Act establishes Congress' right to request PCII, and DHS is and will continue to be responsive to such requests. While the PCII Program's partners are aware that Congress has the right to view PCII, Congressional PCII end-users should be made aware of the legal protections associated with PCII and handle the information in a manner consistent with the privileges and protections provided to PCII by the CII Act. The PCII Program relies on the proper application of PCII handling and safeguarding requirements in order to maintain submitters' trust in the PCII Program. As such, DHS asks that Congressional users take PCII Authorized User Training and acknowledge their roles and responsibilities in safeguarding PCII. Further detailed guidance for Congressional users can be obtained from the PCII Program Procedures Manual.

3. Responsibilities:
   A. DHS will:
      (i) Provide Members of Congress and Congressional staff access to PCII in their capacity as members of a Congressional committee;
      (ii) Provide Authorized User training to Congressional staff for the purposes and under the conditions outlined in this Acknowledgement;
      (iii) Inform the submitter of the PCII, or the person or entity on whose behalf the information was submitted, before that information is disclosed to the Congressional Authorized User;
      (iv) Offer Authorized User Training to Congressional users of PCII;
      (v) Provide copies of the CII Act, the Regulation, and other written guidance, including a copy of the PCII Program Procedures Manual; and

---

1 Subtitle B of Title II of the Homeland Security Act of 2002, Public Law 107-296 , 116 Statute 2135 (6 U.S.C. §131-134).

2 § 214(a)(1)(D)(I) of the Critical Infrastructure Information Act of 2002.

3 6 Code of Federal Regulations, Part 29, as amended. Also known as *Procedures for Handling Protected Critical Infrastructure Information; Final Rule*.

4 6 C.F.R. 29.8(f)(i)(C).

(vi) Provide guidance and assistance regarding PCII handling and safeguarding procedures.

B. The Authorized User acknowledges the following:
(i) The Authorized User agrees to comply with the CII Act, the Regulation, the PCII Program Procedures Manual, and other relevant guidance issued by the PCII Program Manager;
(ii) The Authorized User acknowledges that PCII may only be used and disclosed for the purposes set forth in the CII Act and the Regulation, and will not be used for regulatory purposes or in civil litigation;
(iii) The Authorized User agrees to acknowledge receipt of any PCII he or she receives by signing an acknowledgement form (see Appendix A). Such acknowledgement must include the submission identification number of the PCII. Furthermore, the Authorized User will require any person to whom he or she gives PCII to similarly acknowledge receipt of the PCII and retain a copy of that record;
(iv) The Authorized User acknowledges that PCII markings may not be removed without first obtaining authorization from the PCII Program Manager;
(v) The Authorized User acknowledges that all compromises of PCII and violations of applicable procedures must be reported to DHS;
(vi) Except as provided for in 6 C.F.R. § 29.8(f), or in exigent circumstances, the Authorized User shall not further disclose PCII to any unauthorized party without the prior approval of the PCII Program Office; and
(vii) The Authorized User understands and acknowledges the criminal and administrative penalties established in the CII Act (§ 214(f)) and the Regulation (6 C.F.R. § 29.9(d)) for unauthorized disclosure of PCII.

Note: The PCII Program Manager will keep the original of this document. Copies may be made as necessary. To contact the PCII Program Office:

Telephone: (202) 360-3023
Email: Pcii-info@dhs.gov
Web: www.dhs.gov/pcii

Signed and Acknowledged:

Authorized User

By: _____ (Print Name)
Title: _____
Congressional Office: _____
Phone:
Email:
Signature
Date : _____

Appendix A

RECORD OF RECEIPT OF PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCII)
Date of receipt:
PCII Submission Identification Number:
Delivered by (Print): **Name:** **Title:**
Signature:
Received by (Print): **Name:** **Title:**
Signature:
Office Symbol
Principal Purposes: To provide a receipt for transfer of Protected Critical Infrastructure Information (Subtitle B of Title II of the Homeland Security Act of 2002, Public Law 107-296, 116 Statute 2135 (6 U.S.C. §131-134)). **Routine Uses**: To document transfer of material from courier to a Government Official outside of the PCII Program Office.

Appendix 14 Federal Memorandum of Agreement

Department of Homeland Security

Memorandum of Agreement with Federal Agencies for Access to

Protected Critical Infrastructure Information

1. Parties: The parties to this Memorandum of Agreement (MOA) are the Department of Homeland Security, through its Protected Critical Infrastructure Information Program Office (hereinafter referred to as "DHS"), and _____ (hereinafter referred to as "the Accredited Entity").

2. Purpose: The purpose of this MOA is to set forth the agreed terms and conditions under which DHS will provide Protected Critical Infrastructure Information (PCII) to the Accredited Entity.

3. Authorities: DHS is authorized to enter into this MOA under the Homeland Security Act, 6 U.S.C. §§131-134 and 6 C.F.R. Part 29.

4. Background: The Critical Infrastructure Information Act of 2002 ("CII Act"), Subtitle B of Title II of the Homeland Security Act of 2002, 6 U.S.C. §§131-134, establishes the statutory requirements for the submission and protection of critical infrastructure information. Under 6 U.S.C. § 133(e), DHS is required to establish uniform procedures for the receipt, care, and storage of PCII by Federal agencies. These procedures have been set forth in the Code of Federal Regulations at 6 C.F.R. Part 29. Specifically, 6 C.F.R. 29.8 outlines the requirements for sharing information with Federal agencies and Federal contractors. The PCII Program Office requires that Federal agencies enter into an MOA. This MOA fulfills that requirement. Further detailed guidance can be obtained from the PCII Procedures Manual.

5. Responsibilities:

A. DHS will:

(i) Provide access to PCII to the Accredited Entity for the purposes and under the conditions outlined in this MOA;

(ii) Request and obtain written consent, as applicable, from the person or entity that submitted the information or on whose behalf the information was submitted, before that information is disclosed by the Accredited Entity to an unauthorized party; and

(iii) Train the Accredited Entity's PCII Officer(s) and be available for consultation and guidance.

B. The Accredited Entity will:

(i) Follow all required procedures and regulations to appropriately safeguard and handle PCII;

(ii) Require each of its employees,who will have access to PCII to comply with the statutes, regulations, and rules that address PCII set forth in the CII Act, 6 C.F.R. Part 29, the DHS PCII Procedures Manual, and other relevant guidance issued by the PCII Program Manager, and to periodically check such guidance for updates and amendments;

(iii) Only use PCII for the purposes set forth in the CII Act at 6 U.S.C. §133(a)(1), and, in accordance with 6 C.F.R. 29.3(b), not use PCII for regulatory purposes;

(iv) Designate one or more persons to be PCII Officers. These individuals shall be familiar with and trained in the responsibilities of the PCII Officer as as set forth in 6 C.F.R. 29.4(d), the DHS PCII Procedures Manual, and any other guidance issued by the PCII Program Manager; to include the requirement that PCII markings shall not be removed without first obtaining authorization from the PCII Program Manager.

(v) Consider any violations of procedures regarding PCII as matters subject to rules of conduct (including sanctions) that apply to its employees, and refer violations of 6 U.S.C. § 133(f) or other applicable law to appropriate authorities for prosecution;

(vi) Immediately report all compromises of PCII and violations of applicable procedures to the PCII Program Manager and cooperate with any investigation that may be initiated;

(vii) Not further disclose PCII to any unauthorized party without the prior approval of the PCII Program Manager, except as provided for in 6 C.F.R. § 29.8(f), or in exigent circumstances as provided for in 6 C.F.R. 29.8(e);

(viii) Before sharing with Federal contractors:

(a) Ensure that contractors and subcontractors are performing services in support of the purposes of the CII Act, and have agreed by contract to comply with all of the requirements of the PCII Program;

(b) Ensure that each employee of a consultant, contractor, or subcontractor who will have access to PCII has signed an individual non-disclosure agreement approved of, or provided by, DHS, and is familiar with, will be trained in, and will comply with the provisions of this MOA, the statutes, regulations, and rules that address PCII set forth in the CII Act, 6 C.F.R. Part 29, the DHS PCII Procedures Manual, and other relevant guidance issued by the PCII Program Manager, and will periodically check such guidance for updates and amendments;

(c) Consider any violations of procedures regarding PCII as matters subject to rules of conduct (including sanctions) that apply to its consultants, contractors and subcontractors and refer violations of law to appropriate authorities for prosecution;

(ix) Fully comply with any requests, whether scheduled or unscheduled, by the PCII Program Manager to review the Accredited Entity's compliance with the terms of this MOA, and take any corrective action recommended;

(x) Notify and coordinate with DHS prior to responding to any requests for release of PCII under a court order, agency decision, the Freedom of Information Act, or any other statute or regulation; and

(xi) Forward any submission of CII, received by the accredited entity that is not a part of a categorical inclusion, to the PCII Program Office for validation.

6. Amendments: This MOA is permitted by statute and regulation and required by the PCII Procedures Manual. Should there be a change in any of these authorities, DHS will require conforming amendments to this MOA. This MOA can only be amended by an instrument in writing signed on behalf of both DHS and the Accredited Entity. Such amendments shall be in writing and shall be approved by authorized representatives of DHS and the Accredited Entity.

7. Reimburseables: This MOA does not provide authority for any reimbursable expenditures or funding. In the event that such authorization is required, DHS and the Accredited Entity will,

in a separate agreement, coordinate funding reimbursement through appropriate channels and will execute appropriate Reimbursable Agreements or other funding documents in accordance with the Economy Act and DHS procedures for such agreements including an Economy Act Determination & Findings.

8. Other Provisions: Nothing in this MOA is intended to conflict with current law or regulation. If a term of this MOA is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this MOA shall remain in full force and effect.

9. Effective Date and Termination Provisions: This MOA is effective as of the date of the last required signature. It continues until terminated in writing by either party. It may be terminated effective upon the delivery by any means of written notice of termination signed by an authorized official. Unwillingness by the Accredited Entity to agree to amendments required by DHS will constitute a basis for termination. If terminated, the Accredited Entity agrees to promptly return all PCII that it has received, and any that it has further distributed, to the PCII Program Manager.

10. Original Memorandum of Agreement: The original of this document will be kept by the PCII Program Manager. Copies may be made as necessary.

11. Points of Contact:

DHS:	Accredited Entity:
Name	Name
Phone	Phone
Email	Email

Agreed to and Accepted By:

For The Department of Homeland Security	For _____ (Federal Agency)
By: Laura S. Kimberly	By: _____ (Print Name)
Title: PCII Program Manager	Title: _____
_____	_____
Signature	Signature
_____	_____
Date	Date

Appendix 15 State/Local Memorandum of Agreement

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCII) PROGRAM

MEMORANDUM OF AGREEMENT

Department of Homeland Security Memorandum of Agreement with State Agencies for Access to Protected Critical Infrastructure Information

1. Parties: The parties to this Memorandum of Agreement (MOA) are the Department of Homeland Security, through its Protected Critical Infrastructure Information Program Office (hereinafter referred to as "DHS"), and the _____ (hereinafter referred to as the "Recipient").

2. Authorities: DHS and the Recipient are authorized to enter into this MOA under the Critical Infrastructure Information Act of 2002, Subtitle B of Title II of the Homeland Security Act of 2002, 6 U.S.C. §§131-134 ("CII Act"), and 6 C.F.R. Part 29.

3. Purpose: The purpose of this MOA is to set forth the agreed terms and conditions under which Protected Critical Infrastructure Information (PCII) is provided to the Recipient. The CII Act, establishes the statutory requirements for the submission and protection of critical infrastructure information ("CII"). Under 6 U.S.C. § 133(e), DHS is required to establish uniform procedures for the receipt, care, and storage of PCII. These procedures have been set forth in the Code of Federal Regulations ("C.F.R.") at 6 C.F.R. Part 29. Specifically, 6 C.F.R. 29.8 outlines the requirements for sharing information with State and local government agencies and contractors. 6 C.F.R. 29.8(b) requires a State or local government entity to enter into an arrangement with DHS providing for compliance with 6 C.F.R. Part 29 and acknowledging the understanding and responsibilities of the recipient entity. The PCII Program Procedures Manual provides further guidance, and requires that State and local agencies that obtain PCII from and through the PCII Program Manager (PM) enter into an MOA. This MOA fulfills that requirement.

4. Responsibilities:

A. DHS will:

(i) Accredit the Recipient and appoint a PCII Officer, provided that the entity has satisfied the accreditation requirements set forth in Section 4.B.(ii) below.

(ii) Provide access to PCII to the Recipient for the purposes set forth in the CII Act and under the conditions outlined in this MOA;

(iii) Validate and mark CII and disseminate it to the Recipient;

(iv) Obtain written consent, as necessary, from the person or entity that submitted the information or on whose behalf the information was submitted, before that information is disclosed by the Recipient to an unauthorized party or for an unauthorized use;

(v) Provide applicable procedures and guidelines for the receipt, safeguarding, handling and dissemination of PCII;

(vi) Train the Recipient's PCII Officer(s) and be available for consultation and guidance;

(vii) Provide content and format for training of individuals seeking authorization to access PCII;

(viii) Assist the Recipient in issuing any alerts, advisories and warnings that require DHS' prior approval as set forth in 6 C.F.R. 29.8(e); and

(ix) Notify the Recipient's PCII Officer(s) each time the agency revises or issues new guidance regarding procedures for the receipt, care, storage or use of PCII.

B. The Recipient will:

(i) Require each of its employees and contractors who will have access to PCII to be familiar with, to be trained in, and to comply with, the statutes, regulations, and rules that address PCII set forth in the CII Act, 6 C.F.R. Part 29, the DHS PCII Program Procedures Manual, and other relevant guidance issued by the PCII Program Manager, and to periodically check such guidance for updates and amendments;

(ii) Use its best efforts and cooperate with the PCII Program Office to become accredited as expeditiously as possible, by:

(a) Submitting an application
(b) Signing this MOA
(c) Nominating a PCII Officer
(d) Ensuring that the PCII Officer complete his or her training
(e) Completing the self-inspection plan in conjunction with Standard Operating Procedures for safeguarding, handling and disseminating PCII
(f) Ensuring that the PCII Officer certifies any contractors
(g) Ensuring that any contractors sign a Non-Disclosure Agreement in the form prescribed by the PCII Program Office

(iii) Use any PCII provided to it only for the purposes set forth in the CII Act at 6 U.S.C. §133(a)(1), and, in accordance with 6 C.F.R. 29.3(b), not use PCII for regulatory purposes without first contacting the PCII Program Office;

(iv) Nominate one or more persons to be PCII Officers, all of whom shall be familiar with and trained in the receipt, safeguarding, handling and dissemination requirements for PCII as set forth in 6 C.F.R. Part 29, the DHS PCII Program Procedures Manual, and any other guidance issued by the PCII PM;

(v) Ensure that any employees required by DHS to undergo a background check pursuant to 6 C.F.R. 29.7(b) submit any required paperwork to, and cooperate with, DHS;

(vi) Upon request from DHS, immediately take such steps as may be necessary to return promptly all PCII, including copies, however made, to DHS;

(vii) Consider any violations of procedures regarding PCII as matters subject to rules of conduct (including sanctions) that apply to its employees, and refer violations of the CII Act and 6 C.F.R. Part 29 or other applicable law to appropriate authorities for prosecution, including any administrative, disciplinary, civil, or criminal action, as appropriate, under the laws, regulations and directives of the Recipient's jurisdiction;

(viii) Immediately report all compromises of PCII and violations of applicable procedures to the PCII PM and cooperate with any investigation that may be initiated;

(ix) Ensure that

(a) information it receives from DHS that is marked "Protected Critical Infrastructure Information", is controlled as required, and is used only for allowed purposes (i.e., securing critical infrastructure or protected systems; analysis; warning; interdependency study; recovery; reconstitution; or toehr appropriate purposes, including without limitation, the identification, analysis, prevention, preemption, and/or disruption of terrorist threats to the homeland); and
(b) records of disclosure of PCII are maintained within that entity, as appropriate and that any PCII markings shall not be removed without first obtaining authorization from the PCII PM;

(x) Except as provided for in 6 C.F.R.29.8(f), or in exigent circumstances as provided for in 6 C.F.R. 29.8(e), not further disclose PCII to any other party without the prior approval of the PCII Program Manager;

(xi) Before sharing with contractors:

(a) Certify that contractors and subcontractors are performing services in support of the purposes of the CII Act;
(b) Ensure that each employee of a consultant, contractor, or subcontractor who will have access to PCII has signed an individual non-disclosure agreement approved of, or provided by, DHS, and is familiar with, will be trained in, and will comply with the provisions of this MOA, the statutes, regulations, and rules that address PCII set forth in the CII Act, 6 C.F.R. Part 29, the DHS PCII Program Procedures Manual, and other relevant guidance issued by the PCII PM; and
(c) Consider any violations of procedures regarding PCII as matters subject to rules of conduct (including sanctions) that apply to its consultants, contractors and subcontractors and will refer violations of law to appropriate authorities for prosecution.

(xii) Ensure that contractors have agreed by contract to comply with all of the requirements of the PCII Program;

(xiii) Fully comply with any requests, whether scheduled or unscheduled, by the PCII PM to review the Recipient's compliance with the terms of this MOA, and take any corrective action recommended;

(xiv) Forward any submission of CII received by the Recipient to the PCII Program Office for validation;

(xv) Enter into any Agreements to Operate and/or System Requirements Documents required by the PCII Program Office; and

(xvi) Notify and coordinate with DHS prior to responding to any requests for release of PCII under a court order, agency decision, the Freedom of Information Act, or any other statute or regulation, including similar State and local disclosure laws that apply in the Recipient's jurisdiction.

5. Amendments: This MOA is permitted by statute and regulation and required by the PCII Program Procedures Manual. Should there be a change in any of these authorities, DHS will require conforming amendments to this MOA. This MOA can only be amended by an instrument in writing signed on behalf of both DHS and the Recipient. Such amendments shall be in writing and shall be approved by authorized representatives of DHS and the Recipient.

6. Reimburseables: This MOA does not provide authority for any reimburseable expenditures, or funding. In the event that such authorization is required, DHS and the Recipient will, in a separate agreement, coordinate funding reimbursement through appropriate channels and will execute appropriate Reimbursable Agreements or other funding documents in accordance with the Economy Act and DHS procedures for such agreements including an Economy Act Determination & Findings.

7. Other Provisions: Nothing in this MOA is intended to conflict with current law or regulation. If a term of this MOA is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this MOA shall remain in full force and effect.

8. Effective Date and Termination Provisions: This MOA is effective as of the date of the last required signature. It continues until terminated in writing by either party. It may be terminated effective upon the delivery by any means of written notice of termination signed by an authorized DHS official or Recipient official. Unwillingness by the Recipient to agree to amendments required by DHS will constitute a basis for termination. If terminated, the Recipient agrees to promptly return all PCII that it has received to the PCII PM.

9. Original Memorandum of Agreement: The original of this document will be kept by the PCII PM. Copies may be made as necessary.

10. Points of Contact:

DHS:	Recipient:
Name	Name
Phone	Phone
Email	Email

Agreed to and Accepted By:

For The Department of Homeland Security	For _____ (State Agency)
By: Laura L.S. Kimberly	By: _____ (Print Name)
Title: PCII Program Manager	Title: _____
_____ Signature	_____ Signature
_____ Date	_____ Date

Appendix 16 Non-Disclosure Agreement

DEPARTMENT OF HOMELAND SECURITY

NON-DISCLOSURE AGREEMENT FOR PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCII)

I, _____, an individual official, employee, consultant, or subcontractor of or to _____(the Authorized Entity), intending to be legally bound, hereby consent to the terms in this Agreement in consideration of my being granted conditional access to certain information, specified below, that is owned by, produced by, or in the possession of the United States Government.

I hereby acknowledge that I am familiar with, and I will comply with all requirements of the Protected Critical Infrastructure Information (PCII) program set out in the Critical Infrastructure Information Act of 2002 (CII Act), (Title II, Subtitle B, of the Homeland Security Act of 2002, Public Law 107-296, 196 Stat. 2135, 6 U.S.C. 101 et seq.), as amended, the implementing regulations thereto (6 C.F.R. Part 29), as amended, and the applicable PCII Procedures Manual, as amended, and with any such requirements that may be officially communicated to me by the PCII Program Manager or the PCII Program Manager's designee.

I hereby acknowledge that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of the PCII to which I am granted access as cited in this Agreement and in accordance with the guidance provided to me relative to the PCII.

I understand and agree to the following terms and conditions of my access to PCII indicated above:

1. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of PCII to which I have been provided conditional access, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing PCII have been approved for access to it, and that I understand these procedures.

2. By being granted conditional access to PCII, the United States Government has placed special confidence and trust in me and I am obligated to protect this information from unauthorized disclosure, in accordance with the terms of this Agreement and the laws, regulations, and directives applicable to PCII to which I am granted access.

3. I acknowledge that I understand my responsibilities and that I am familiar with and will comply with the standards for protecting such information that I may have access to in accordance with terms of this Agreement and the laws, regulations and/or directives, applicable to the information to which I am granted access. I understand that DHS may conduct inspections of my place of business pursuant to established procedures for the purpose of ensuring compliance with the conditions for access, dissemination, handling and safeguarding of PCII under this Agreement.

4. I will not disclose or release any PCII provided to me pursuant to this Agreement without proper authority or authorization. Should situations arise that warrant the disclosure or release of such PCII, I will do so only under approved circumstances and in accordance with the laws, regulations, or directives applicable to the PCII. I will honor and comply with any and all dissemination restrictions cited to me by the proper authority.

5. (a) Upon the completion of my engagement as an employee, consultant, or subcontractor under the contract, or the completion of my work on the PCII Program, whichever occurs first, I will surrender promptly to the PCII Program Manager or the Program Manager's designee, or to the appropriate PCII officer, PCII of any type whatsoever that is in my possession.

(b) If the Authorized Entity is a United States Government contractor performing services in support of the PCII Program, I will not request, obtain, maintain, or use PCII unless the PCII Program Manager or Program Manager's designee has first made in writing, with respect to the contractor, the certification as provided for in Section 29.8(c) of the implementing regulations to the CII Act, as amended.

6. I hereby agree that I will not alter or remove markings, which indicate a category of information or require specific handling instructions, from any material I may come in contact with, unless such alteration or removal is authorized by the PCII Program Manager or the PCII Program Manager's designee. I agree that if I use information from a sensitive document or other medium, I will carry forward any markings or other required restrictions to derivative products, and will protect them in the same matter as the original.

7. I hereby agree that I shall promptly report to the appropriate official, in accordance with the guidance issued for PCII, any loss, theft, misuse, misplacement, unauthorized disclosure, or other security violation that I have knowledge of, whether or not I am personally involved. I also understand that my anonymity will be kept to the extent possible when reporting security violations.

8. If I violate the terms and conditions of this Agreement, such violation may result in the cancellation of my conditional access to the information covered by this Agreement. This may serve as a basis for denying me conditional access to other types of information, to include classified national security information.

9. With respect to PCII, I hereby assign to the entity owning the PCII and the United States Government, all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of PCII not consistent with the terms of this Agreement.

10. This Agreement is made and intended for the benefit of the United States Government and may be enforced by the United States Government or the Authorized Entity. By granting me conditional access to information in this context, the United States Government and, with respect to PCII, the Authorized Entity, may seek any remedy available to it to enforce this Agreement, including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I understand that if I violate the terms and conditions of this

Agreement, I could be subjected to administrative, disciplinary, civil, or criminal action, as appropriate, under the laws, regulations, or directives applicable to the category of information involved and neither the United States Government nor the Authorized Entity have waived any statutory or common law evidentiary privileges or protections that they may assert in any administrative or court proceeding to protect any sensitive information to which I have been given conditional access under the terms of this Agreement.

11. Unless and until I am released in writing by an authorized representative of the Department of Homeland Security, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time that I am granted conditional access, and at all times thereafter.

12. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions shall remain in full force and effect.

13. My execution of this Agreement shall not nullify or affect in any manner any other secrecy or non-disclosure Agreement which I have executed or may execute with the United States Government or any of its departments or agencies.

14. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 12958, as amended; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents); and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. 783 (b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.

15. Signing this Agreement does not bar disclosures to Congress or to an authorized official of an executive agency or the Department of Justice that are essential to reporting a substantial violation of law.

16. I represent and warrant that I have the authority to enter into this Agreement.

17. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the brief officer has made available to me any laws, regulations, or directives referenced in this document so that I may read them at this time, if I so choose.

DEPARTMENT OF HOMELAND SECURITY
NON-DISCLOSURE AGREEMENT
Acknowledgment

Typed/Printed Name:	Government/Department/Agency/Business Address	Telephone Number:

I make this Agreement in good faith, without mental reservation or purpose of evasion.

Signature: Date:

WITNESS:

Typed/Printed Name:	Government/Department/Agency/Business Address	Telephone Number:

Signature: Date:

Appendix 17 Contractor Certification Memorandum for the Record

MEMORANDUM FOR THE RECORD

FROM: Laura Kimberly
Program Manager, PCII Program Office, NPPD, DHS

DATE: <Date>

SUBJECT: Certification of <Contractor Name> – <Task Order>

This memorandum is to certify that <Contractor Name> and its subcontractors are engaged in activities in support of the <Name of Government Entity> as authorized users of Protected Critical Infrastructure Information (PCII) under the provisions of 6 Code of Federal Regulations Part 29 (29.8(c)). <Contractor Name> is providing essential services to <Name of Government Entity>. As such, employees of <Contractor Name> and its subcontractors may access PCII in the performance of their tasks. As required under the regulation, the current <Contractor Name> contract under which it may have access to PCII, <Contract Number>, <Task Order>, has been or will be modified to include approved language authorizing <Contractor Name> to access PCII and documenting <Contractor Name>'s agreement to comply with all PCII program requirements. All <Contractor Name> employees and subcontractors performing services for <Name of Government Entity> under this contract shall sign the approved PCII Program's Non-Disclosure Agreement and attend all required PCII training prior to having access to PCII.

_____
Laura Kimberly

cc: <PCII Officer>,
<Contractor POC>, <Contractor Name>

MEMORANDUM FOR THE RECORD

FROM [Contractor being certified]

TO: PCII Program Office

DATE:

SUBJECT: Certification of Contractors Supporting [operation being supported]

[Government entity seeking contractor certification] certifies that the following contractors and subcontractors are engaged in activities in support of the <Name of Government Entity> as authorized users of Protected Critical Infrastructure Information (PCII) under the provisions of 6 Code of Federal Regulations Part 29 (29.8(c)).

Company	Contract Number	Name & Contact Information of COTR

The contractors and subcontractors listed above are providing essential services to <Name of Government Entity>. As such, their employees shall receive appropriate PCII training and sign the PCII Program's Non-Disclosure Agreement (NDA). As required under the regulation, their contracts has been, or will be, modified to include approved language authorizing them to access PCII and documenting their agreement to comply with all PCII program requirements.

Appendix 18 Contract Modification Language

Non-Disclosure of Protected Critical Infrastructure Information

The parties agree to comply with the Final rule promulgating regulations at Title 6 Code of Federal Regulations Section 29 to govern procedures for handling critical infrastructure information. The regulations detailed in the Final rule, which was effective upon publication pursuant to Section 808 of the Congressional Review Act, were promulgated pursuant to Title II, Section 214 of the Homeland Security Act of 2002, known as the "Critical Infrastructure Information Act of 2002" (CII Act).

The Contractor shall not request, obtain, maintain or use Protected Critical Infrastructure Information (PCII) without a prior written certification from the PCII Program Manager or a PCII Officer that conforms to the requirements of Section 29.8(c) of the Final Rule.

The Contractor shall comply with all requirements of the PCII Program set out in the CII Act, in the implementing regulations published in the Final Rule, and in the PCII Procedures Manual as they may be amended from time to time, and shall safeguard PCII in accordance with the procedures contained therein.

The Contractor shall ensure that each of its employees, consultants, and subcontractors who work on the PCII Program have executed Non-Disclosure Agreements (NDAs) in a form prescribed by the PCII Program Manager and agrees that none of its employees, consultants or sub-contractors will be given access to PCII without having previously executed an NDA.

Appendix 19 PCII Loss or Misuse Report

PCII LOSS OR MISUSE REPORT

1.	Name of Entity							
2.	Address of Entity							
	Street							
	City							
	State							
	ZIP							
3.	Name of PCII Program Officer							
4.	PCII Program Officer Contact Information							
	Phone		FAX					
5.	Are you reporting loss or misuse of PCII?			Loss of PCII				
				Misuse of PCII				
6.	Is the loss/misuse actual or suspected?			Actual				
				Suspected				
7.	What PCII was lost or misused?			Tracking Number				
	Description of content							
9.	When was the PCII lost or misused?		Date					
8.	Who was the last person or entity to use the PCII that was lost or misused?							
9.	What form was the PCII?	EMAIL	DISK	HARD COPY	AUDIO	VIDEO	OTHER	
10.	Was the loss/misuse immediately reported to the Accreditation Management Team?			YES				
				NO				
11.	When did the PCII Officer first become aware of the loss or misuse of PCII?		Date					
12.	How did the PCII Officer become aware of the loss or misuse of PCII?							
13.	Print name of individual preparing the report							
14.	Signature of individual preparing the report							

DHS Form 9018 (1-08) Page 1 of 1

- End-