PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCII) PROGRAM

FREQUENTLY ASKED QUESTIONS

WHAT IS THE PCII PROGRAM?

The PCII Program, part of the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD), is an information-protection program to enhance information sharing between the private sector and the government. Qualifying information voluntarily submitted to the government and validated as PCII is protected from public disclosure under the Freedom of Information Act (FOIA) and similar State and local disclosure laws, and use in civil litigation.

DHS and other Federal, State and local analysts use PCII in pursuit of a more secure homeland, focusing primarily on:

- Analyzing and securing critical infrastructure and protected systems;
- Identifying vulnerabilities and developing risk assessments; and
- Enhancing recovery preparedness measures.

PCII can be shared directly through the PCII Program Office or through DHS field representatives and other Federal agencies designated to receive PCII by the PCII Program Manager.

WHAT PROTECTIONS ARE OFFERED BY THE PCII PROGRAM?

All information designated as PCII is protected throughout its lifecycle. PCII Program safeguards ensure PCII is:

- Accessed only by authorized and properly trained individuals;
- Used appropriately for analysis of threats, vulnerabilities and other homeland security purposes;
- Protected from disclosure under the Freedom of Information Act (FOIA) and similar State and local disclosure laws; and
- Not used directly in civil litigation nor as the basis for regulatory action.

This protection extends to drafts and copies of the PCII retained by the submitter(s) or person working with the submitter(s), as well as any discussions with DHS regarding the PCII.

WHAT ARE THE RESPONSIBILITIES OF THE PCII PROGRAM OFFICE?

Once the Program Office validates submitted information as PCII, its mission is to facilitate access to and safeguard PCII. The PCII Program Office's responsibilities also include: establishing guidelines for handling, using, and storing PCII; training users and recipients on safeguarding PCII; and accrediting government entities to handle PCII.

WHAT IS THE DEFINITION OF CRITICAL INFRASTRUCTURE INFORMATION (CII)?

(CII) is information not customarily in the public domain[1] and related to the security of critical infrastructure or protected systems, including documents, records or other information concerning:

- Actual, potential, or threatened interference with, attack on, compromise or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct that violates Federal, State, local, or tribal 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.

For further information on CII, please see the Critical Infrastructure Information Act of 2002 (CII Act) and "Procedures for Handling Infrastructure Information; Final Rule" (6 CFR Part 29) available at www.dhs.gov/pcii.

WHAT ARE THE REQUIREMENTS FOR ACCESSING PCII?

PCII is made available only to those Federal, State and local government employees and their contractors who:

- Are trained in the proper handling and safeguarding of PCII;
- Have homeland security responsibilities as specified in the CII Act, the Final Rule, and policies and procedures issued by the PCII Program Office;
- Have a need to know the specific information; and
- Sign a Non-Disclosure Agreement (non-Federal employees).

In addition to the above requirements, government contractors must modify relevant contracts to comply with requirements of the PCII Program. The contract modification is not a prerequisite to accessing PCII; however, the contractor must contractually acknowledge its responsibilities with respect to PCII as soon as practicable. To avoid delay or interruption of access to PCII, contractors can be certified by the PCII Program Manager or a PCII Officer.

The PCII Accreditation Program is in place to ensure consistent application of uniform program standards and requirements by all participating entities.

[1] *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.''

WHAT ARE THE PENALTIES FOR INTENTIONALLY MISHANDLING PCII?

Recognizing that receipt of CII submissions from the private sector is contingent upon keeping submissions safe from unauthorized access, distribution, and misuse, the CII Act and the Final Rule apply criminal and civil penalties for intentionally mishandling PCII.

All Federal, State and local government employees with access to PCII, including the PCII Program Manager, all PCII Program staff, PCII Officers and Deputy Officers, and all Designees of the PCII Program Manager share responsibility for ensuring that PCII is properly safeguarded in accordance with stringent procedures. Federal, State and local government employees who do not follow these safeguarding procedures may be subject to disciplinary action including criminal and civil penalties and loss of employment. State laws governing theft, conspiracy and trade secrets may apply to government employees and contractors who intentionally mishandle PCII. The CII Act does not limit any enforcement mechanism.

WHO CAN SUBMIT INFORMATION TO THE PCII PROGRAM OFFICE?

Individuals or entities who have information about a critical infrastructure that is not customarily in the public domain, as defined by the CII Act and the Final Rule, can provide such information to the PCII Program Office, so long as the information is submitted in good faith and is not submitted in lieu of compliance with any regulatory requirement.

Entities that might submit information include, but are not limited to:

- Private sector companies;
- Working groups comprised of government and private sector representatives; and
- State and local government entities.

WHAT TYPES OF INFORMATION-SHARING PARTNERSHIPS AND PROGRAMS CAN BENEFIT FROM THE PCII PROGRAM?

The PCII Program provides protections used in various public/private critical infrastructure information-sharing programs, both within DHS and in other agencies. Information-sharing programs within DHS include:

- National Cyber Security Division's United States Computer Emergency Readiness Team (US-CERT) Secure Portal Submissions Capability
- Infrastructure Information Collection Division's Constellation/Automated Critical Asset Management System (C/ACAMS)
- Protective Security Coordination Division's Site Assistance Visits (SAVs) and Buffer Zone Plans (BZPs)

WHAT MUST ACCOMPANY A SUBMISSION TO QUALIFY FOR PROTECTION?
Submitters are encouraged to contact the PCII Program Office at (202) 360-3023 or pcii-info@dhs.gov prior to submitting their information to ensure that the Program Office can accept the submission format and for any additional guidance.

Two items must be included with information submitted for PCII protection under the CII Act:

- An Express Statement requesting the protection offered by the CII Act; and
- A Certification Statement including the submitter's contact information and certifying that the information is not customarily in the public domain.

When accompanied by an Express Statement and a signed Certification Statement, the submission will be granted the presumption of protection throughout the entire process. If the Certification Statement is incomplete, the PCII Program Office will request that the submitter provide a complete Certification Statement within 30 calendar days of the submitter's receipt of the request. If the submitter does not remedy the deficiency within 30 days of the request, the PCII Program Office will either return the information to the submitter in accordance with the submitting person or entity's written preference or destroy the submission in accordance with the Federal Records Act and Department of Homeland Security regulations.

All submissions are assigned an identification number that must be included on all original PCII, copies of original PCII and products created from PCII.

DOES THE PCII PROGRAM HAVE WAYS OF EXPEDITING THE ACCEPTANCE OF PRESUMPTIVELY VALID INFORMATION?
Yes. 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. CII within 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 includes an Express Statement and the PCII Program Office has pre-validated that type of information as PCII. The PCII Program Manager must appoint a Designee before an entity can establish a categorical inclusion. Moreover, only Federal entities or systems or programs managed and overseen by a Federal employee can make use of the categorical inclusion. Interested parties should coordinate with the PCII Program Office to establish a categorical inclusion and complete any required documentation.

DO SUBMISSIONS HAVE TO GO DIRECTLY TO THE PCII PROGRAM OFFICE?

The Final Rule identifies procedures for indirect submissions to DHS through DHS field representatives and other Federal agencies. The PCII Program Manager designates Federal employees to receive CII on behalf of DHS, but only the PCII Program Manager is authorized to make the decision to validate a submission as PCII. Those designated to receive CII on behalf of DHS must be Federal employees. The PCII Program Manager decides who may be a Designee, and functions to be delegated to that Designee are determined on a case-by-case basis. All Designees are trained to ensure compliance with the requirements of the Final Rule. The PCII Program Office maintains a record of all indirect submissions and the associated metadata through the PCII Program Management System (PCII MS).

WHO CAN MARK INFORMATION AS PCII?

Only the PCII Program Office or a PCII Program Manager Designee may mark information as PCII and provide it with a submission identification number. Information that does not contain the requisite PCII markings and identification number is not PCII. The PCII marking remains until the PCII Program Office determines that the information no longer qualifies for PCII protection or the submitter requests that the protection be removed.

PCII Authorized Users must ensure products created from PCII include a PCII cover sheet and are marked with "Protected Critical Infrastructure Information" in the headers and footers to alert users to the information's status and protection requirements.

WHAT SHOULD I DO IF I RECEIVE MATERIAL MARKED AS PCII BUT IT DOES NOT HAVE A SUBMISSION IDENTIFICATION NUMBER?

All information that is Protected Critical Infrastructure Information (PCII) must be marked with "Protected Critical Infrastructure Information" in the headers and footers of the documentation and labeled with the protection statement available on the PCII Web site. In addition, all PCII must have a submission identification number. If the information does not have a submission identification number, please contact the PCII Program Office immediately at (202) 360-3023 or at pcii-info@dhs.gov

CAN INFORMATION BE BOTH PCII AND SENSITIVE SECURITY INFORMATION (SSI)?

Yes. Information can be both PCII and SSI. According to the SSI regulation at 49 CFR Part 1520.15(h), disclosure of information that is both SSI and PCII is governed solely by the PCII requirements of the Critical Infrastructure Information Act of 2002. Therefore, users handling materials that are marked as both PCII and SSI should observe all PCII handling, safeguarding and dissemination requirements.

WHAT IS CONTROLLED UNCLASSIFIED INFORMATION (CUI) AND HOW DOES IT IMPACT PCII?

On May 9, 2008, the President released the Memorandum for the Heads of Departments and Agencies on the designation and sharing of Controlled Unclassified Information (CUI). The Presidential Memorandum institutes CUI as the single, categorical designation throughout the executive branch for all information within the scope of that definition, which includes most information referred to as 'Sensitive But Unclassified' (SBU). The Memorandum also establishes a corresponding new CUI Framework for designating, marking, safeguarding and disseminating information designated as CUI.

PCII is an exception to the CUI framework as explicitly stated in the Memorandum. PCII will retain its handling, safeguarding and dissemination requirements. PCII, however, will be subject to the CUI governance processes and all PCII specific safeguarding and dissemination requirements will be listed in the CUI Registry. The CUI framework remains in its initial implementation phase and there is no CUI Registry yet. More information about the CUI framework can be found at www.archives.gov and www.ise.gov.