

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION PROGRAM

I. Purpose

This Directive sets forth the policy and procedures for submission, validation, dissemination, safeguarding, and handling of Protected Critical Infrastructure Information (PCII), voluntarily shared by private sector with government entities for purposes of homeland security.

II. Scope

This Directive applies throughout DHS, to all offices, divisions, bureaus, as well as the officers, members, employees, detailees, contractor personnel or others that access, use, and disseminate PCII.

III. Authorities

- A. Title II, Subtitle B, of the Homeland Security Act of 2002, Public Law 107-296, 116 Statute 2135 (Title 6, United States Code (U.S.C.) 131 et seq.), the Critical Infrastructure Information Act of 2002 (CII Act), Public Law 107-296, §§ 211-215, 116 Stat. 2135, 2150-55 (codified as amended at Title 6 U.S.C. §§ 131–134)
- B. Executive Order 13526, “Classified National Security Information”
- C. Title 6, Code of the Federal Regulations (CFR), Part 29, “Procedures for Handling Critical Infrastructure Information”
- D. Management Directive 11042.1, “Safeguarding Sensitive but Unclassified (For Official Use Only) Information”
- E. PCII Program Procedures Manual dated April 2009 and any amendments thereto (available at www.dhs.gov/pcii) (Manual)

IV. Responsibilities

- A. The ***PCII Program Manager***. Is designated by the Under Secretary for the National Protection and Programs Directorate (formerly Information Analysis and Infrastructure Protection); and implements the Nationwide PCII Program and oversees

Federal and non-Federal actions to comply with the CII Act and 6 CFR Part 29.

B. **Key PCII Program Officials:**

1. **PCII Officer:** An employee or contractor of a federal, state, local, tribal or territorial government entity appointed by their entities to manage and oversee PCII Program responsibilities within their entities. The PCII Program Manager approves all appointments and all PCII Officers take training to become certified as PCII Officers.

2. **PCII Program Manager Designee:** Federal personnel outside of the PCII Program Office appointed by the PCII Program Manager, who administers and manages a specific PCII categorical inclusion; process whereby certain subject matter or types of information are categorically protected as PCII, and establishes specific procedures for the receipt and processing of such information. The PCII Program Manager Designee ensures that PCII is accessed and handled in accordance with PCII Program policy. For all categorical inclusions, the government entity overseeing the receipt of categorical PCII and the PCII Program Office establishes an agreement to operate which defines the conditions under which that entity receives information.

3. **PCII Authorized User:** A federal, state, local, tribal, or territorial government employee or contractor with homeland security responsibilities, who has a valid need-to-know and has successfully completed the requisite PCII training, and met the access requirements for using PCII. The Authorized User accesses PCII to conduct analysis of the infrastructure to develop risk assessments, interdependency studies, evaluate vulnerabilities or gaps in assets, etc., that are necessary to inform decision-makers about the security and resilience of the Nation's infrastructure. DHS may conduct background investigations of an individual before granting access to any PCII.

V. Policy and Requirements

A. **Receipt, Validation, Marking and Protection of PCII:**

1. In order to be validated as PCII, Critical Infrastructure Information (CII) is voluntarily submitted to the DHS PCII Program with an Express and Certification Statement as described in the CII Act and its implementing rule, 6 CFR Part 29. Information properly submitted is presumptively protected as "Sensitive But Unclassified, (SBU)" PCII until the PCII Program makes a final determination as to the status of the information. Refer to 6 CFR Part 29 for additional details.

2. All CII submitted for protection is reviewed to validate as PCII. See PCII Program Procedures Manual for details

3. Only the PCII Program Manager is authorized to validate and mark information as PCII. All PCII is required to have a submission identification number, "Protected Critical Infrastructure Information" in the header and the footer of each page of the document, labeled with a prescribed PCII protection statement and accompanied with a PCII Cover Sheet. PCII Authorized Users are permitted to create and mark derivative products per the PCII Program Procedures Manual and Works Product Guide.

B. **Safeguarding, Transmitting, and Destroying PCII:**

1. **Safeguarding PCII:** All recipients of PCII, including hard and electronic copies, and derivative work products, are required to safeguard PCII to the fullest extent practicable. PCII is only to be accessed by authorized users who have a need-to-know and who are properly trained in marking, using, storing, reproducing, disseminating, transmitting and destroying PCII. See the PCII Program Procedures Manual for pertinent details.

2. **Transmitting PCII:** The PCII Program Manager and the PCII Program Manager Designee are authorized to provide access to PCII to PCII Authorized Users upon a determination that the access supports homeland security purposes as set forth in 6 C.F.R. part 29, § 29.8. Additionally, the PCII Program Manager or PCII Program Manager Designee may provide PCII to departments and governmental agencies that have executed a Memorandum of Agreement (MOA) with DHS. PCII may be transmitted both internally and externally by mail, fax, e-mail, or wireline or wireless telecommunication. Section 7.3 of the PCII Program Procedures Manual provides specific transmittal requirements. The PCII Program also observes transmission procedures for "Sensitive But Unclassified" information, as identified in DHS MD 11042.1, as long as they align with the requirements established by the PCII Program Manager.

3. **Destruction of PCII:** Only the PCII Program Manager may destroy or authorize the destruction of original PCII. PCII Authorized users can destroy copies of PCII and work products containing PCII. The PCII Program Procedures Manual outlines methods for destruction of PCII.

4. **Requests for PCII by Congress, Government Accountability Office (GAO), and through the Freedom of Information Act (FOIA):** PCII is accessible to Congress, the Government Accountability Office (GAO), or law enforcement agencies conducting criminal investigations upon request. However, PCII is exempt from disclosure under FOIA and other similar state, local, tribal, and territorial disclosure laws. Any PCII Authorized User or PCII Program Officer who receives a FOIA or equivalent State, local, tribal or territorial government request should contact the PCII Program Manager for further guidance.

C. **Use of and Accessing PCII:**

1. **Using PCII:** A PCII Authorized User may use PCII to develop derivative work products, alerts, advisories and warnings.

a. Work products containing PCII are subject to the same handling, storage, and marking requirements as original PCII. Refer to Procedure Manual for detail related to work products.

b. PCII contained in classified documents maintains its protections under the CII Act of 2002 even if the document is later declassified. PCII commingled with classified information complies with all marking requirements of both PCII and the highest level of classification with which it is commingled, and retains its PCII markings on each page and be portion marked as necessary.

PCII cover sheets are placed directly behind the classified cover sheet, and a PCII limited distribution statement are footnoted to all PCII paragraphs (linking the distribution statement with the PCII information, and pages containing PCII has the relevant Submission Identification Numbers for all PCII used on that page.

c. DHS Components using PCII to prepare advisories, alerts, and warnings for dissemination to non-PCII Authorized Users are required to sanitize PCII information traceable to the submitter consistent with the Guide for PCII Work Products.

2. **One-time or Emergency Access to PCII:** A federal, state, local, tribal, or territorial government employee or contractor requiring, in exigent circumstances, access to PCII before completing PCII Authorized User training may do so on a one-time basis, including during meetings, by adhering to the following protocols:

a. The PCII holder confirms that the recipient has a valid need-to-know.

b. Comply with handling and safeguarding terms/conditions outlined in Categorical Inclusion ATOs, non-disclosure agreements (NDA); DHS Form 9017 (10-07), and MOAs, executed with the DHS PCII Program Office.

c. Recipient acknowledges that the PCII Cover Sheet is satisfying the NDA requirements for one-time access to PCII.

d. All individuals, including those with a one-time access to PCII are subject to safeguarding and handling requirements and penalties associated with PCII as outlined in the PCII Cover Sheet and related guidance.

e. The recipient completes PCII Authorized User Training within 30 calendar days of receiving access to PCII as instructed on the PCII Cover Sheet, and officially registers in the Protected Critical Infrastructure Information Management System (PCIIMS); system of record for managing PCII authorized users.

D. **Oversight & Violations of PCII Program Procedures:**

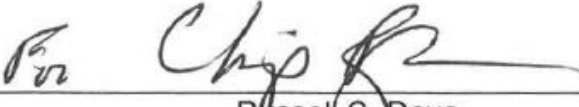
1. **Oversight of PCII Programs:** The PCII Program Manager executes oversight and compliance duties which includes: PCII Officer(s) undertaking self-inspections of their PCII programs, site visits and system audits as necessary for managing, training, handling, storing, sharing, and marking PCII.

2. **Violations, Reporting and Investigative PCII Procedures:** A violation is any unauthorized disclosure or use of PCII. Any suspected or actual violation of security procedures is immediately be reported to the PCII Officer, Program Manager or Designee for further action.

3. **Penalties:** As established in section 214(f) of the CII Act of 2002, anyone who knowingly publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law, any CII protected from disclosure, are fined under title 18 of the United States Code, imprisoned not more than 1 year, or both, and be removed from office or employment. The PCII Program Manager may also disqualify or remove any person or entity from the Program who violates PCII procedures, uses PCII inappropriately, or breaches PCII agreements.

VI. Questions

For additional information about the PCII Program and its procedures, please contact the PCII Program Manager at pcii-info@hq.dhs.gov or call (866) 844-8163



Russel C. Deyo
Under Secretary for Management

FEB 29 2016

Date