

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

Requirements for Use

N o n d i s c l o s u r e

This document contains Protected Critical Infrastructure Information (PCII). In accordance with the provisions of the Critical Infrastructure Information Act of 2002 (the "CII Act"), (6 U.S.C. §671- 674), 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. Safeguard and disseminate 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 not a PCII Authorized User, you are required to complete the training within 30 days of receipt of this information.

Go to <https://www.cisa.gov/pcii-authorized-user-training> for training. Contact pcii-assist@cisa.dhs.gov for assistance.

A c c e s s

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

- Assigned to homeland security duties related to this critical infrastructure;
- Demonstrate a valid need-to-know; and
- Sign a Non-Disclosure Agreement (except Federal employees).

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

H a n d l i n g

Storage: When not in your possession, store securely in a locked desk drawer or 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.

Email: If possible encrypt the email. If impractical or unavailable, transmit the PCII using approved email systems according to proper PCII Program handling procedures. Send PCII as a password protected attachment and provide the password in a separate email. Subject line must state: "This email Contains Protected Critical Infrastructure Information (PCII)". Do not place PCII in the body of the email. **Do not send PCII to personal, non-employment related email accounts.**

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 place in a second envelope with 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: If possible use a secure fax. When sending via non-secure fax, coordinate with the recipient to ensure 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.

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

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 computers, delete file and empty recycle bin.

S a n i t i z e d P r o d u c t s

You may use PCII to create a sanitized work product. The product must not reveal any information that:

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

D e r i v a t i v e P r o d u c t s

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 contact the PCII Program Office.

Submission Identification Number:

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION