SHARING PCII

One of the major benefits of the Protected Critical Infrastructure Information (PCII) Program, administered and managed by CISA within DHS, is to assist stakeholders understanding of issues concerning the security of physical and cyber critical infrastructure. The PCII Program encourages participation in security assessments through legally protecting the information voluntarily submitted. More importantly it protects the information as government Homeland Security Analysts share the analysis with other partners. As the means to share information evolve, especially digitally through collaborative tools and email, protecting PCII from inadvertent disclosure must be a focus of PCII Authorized Users. The below procedures are designed to provide easy to remember steps.

PRINCIPLES OF SHARING PCII

Check Participants for PCII Authorized User Status

PCII is Sensitive but Unclassified (SBU) information and can be shared accordingly. To handle, view, and/or receive PCII in any form one must be a current PCII Authorized User. To verify PCII Authorized User status, login and use the search function in PCIIMS or email the PCII Program Office at PCII-Assist@cisa.dhs.gov. Verification plus a need-to-know is required before sharing PCII, whether by email, in-person, or virtual meetings.

Ensure PCII is Marked

When sharing a PCII protected document between PCII Authorized Users, ensure the document's first page is an approved green PCII Cover Sheet and all subsequent pages' headers and footers are marked with **PROTECTED CRITICAL INFRASTRUCTURE INFORMATION**.

Delete Copies of PCII When No Longer Required

Once sharing of PCII is no longer required, either destroy through shredding hard copy documents or delete electronic copies. The PCII Program Office authorizes certain systems to store original PCII, but copies are frequently shared in many forms with authorized users. To prevent unauthorized disclosure, ensure PCII is stored either physically or electronically appropriately with proper access controls.

SHARING PCII VIA EMAIL

Follow Guidelines for Emailing PCII

Sharing PCII by email is authorized and convenient. To avoid inadvertent disclosure, follow these procedures:

- Verify an approved green PCII Cover Sheet is the first page of the document.
- Verify document's headers and footers read: **PROTECTED CRITICAL INFRASTRUCTURE INFORMATION**
- Verify all recipients are PCII Authorized Users – beware of distribution lists.
- Enter in email subject line: **THIS EMAIL CONTAINS PROTECTED CRITICAL INFRASTRUCTURE INFORMATION**
- Do NOT place PCII in the body of the email.
- Place the below text in the body of the email:

  *****CONTENTS HEREIN CONTAIN PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCII)*****
  In accordance with the provisions of the 6 U.S.C. § 131 et seq. – The Critical Infrastructure Information Act of 2002 (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. PCII must be safeguarded and disseminated according to the CII Act, 6 C.F.R part 29, and the PCII Program requirements and not disclosed to other individuals without following access requirements. Unauthorized release may result in criminal and administrative penalties.

- Encrypt the email if possible. If encryption is unavailable, password protect the attachment containing PCII and email the password separately.
- Verify recipient(s) received the email containing PCII.

SHARING PCII AT IN-PERSON AND VIRTUAL MEETINGS

Announce the Meeting Will Share PCII

Prior to starting an in-person or virtual meeting, the meeting organizer must first verify all participants are PCII Authorized Users by logging in to PCIIMS or contacting the PCII Program Office. Announce before the meeting starts: **THIS MEETING CONTAINS PROTECTED CRITICAL INFRASTRUCTURE INFORMATION OR PCII.** If an attendee is not a PCII Authorized User but meets eligibility requirements and the situation requires an immediate need (exigent circumstances) for sharing PCII, then they must read, sign and acknowledge the green PCII Cover Sheet and notify the PCII Program Office who will assist them to register and conduct PCII Authorized User training within 30 calendar days of the receipt of the PCII.

Messaging and Chat Functions

Contents in chat and message functions are digitally recorded and subject to disclosure under laws such as FOIA or State and local disclosure or "Sunshine Laws." Meeting participants cannot attach or send documents containing PCII within chat spaces. Upon verification of PCII Authorized User status of meeting participants, displaying PCII documents in the collaborative space (e.g., sharing screen) is permitted. To avoid inadvertent disclosure of PCII, the meeting organizer must insert the below PCII warning in the chat or message window before the meeting commences and upon its conclusion to ensure the information is protected against disclosure.

*****CONTENTS HEREIN MAY CONTAIN PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCII)*** In accordance with the provisions of the 6 U.S.C. § 131 et seq. – The Critical Infrastructure Information Act of 2002 (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. PCII must be safeguarded and disseminated according to the CII Act, 6 C.F.R part 29, and the PCII Program requirements and not disclosed to other individuals without following access requirements. Unauthorized release may result in criminal and administrative penalties.**

SANITIZING PCII FOR DISSEMINATION

Federal, State, or local government entities may use PCII to prepare advisories, alerts, and warnings regarding potential threats and vulnerabilities to physical and cyber critical infrastructure for dissemination to individuals outside of the PCII Authorized User community such as public and private sector individuals or foreign governments. When an advisory, alert or warning is produced, the product must be sanitized to remove all PCII. For the purposes of the PCII Program, "sanitization" means distilling the information so 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)*
- *Is otherwise not customarily in the public domain*

SECURE SHARING IS CRITICAL TO HOMELAND SECURITY

The PCII Program's protections enable governments at all levels focused on the security of physical and cyber critical infrastructure to build key relationships with partners by sharing security-related information. The PCII Program enhances the ability to conduct analysis, develop homeland security plans and strategies to reduce security risks, increase the resilience of critical infrastructure, and produce timely and accurate alerts and warnings, as required. With minimal effort, PCII Authorized Users with a need-to-know can rapidly share PCII across multiple digital platforms conveniently and securely by following the above procedures.

CONTACT INFORMATION

To register and train to become a PCII Authorized User please navigate to PCII Management System - Login Form (cisa.gov) and select "Registration" – if any issues please contact the CISA TOC at: TOC@mail.cisa.dhs.gov

For all other PCII Program questions please contact the PCII Program Office at: PCII-Assist@cisa.dhs.gov

For additional information on the PCII Program please visitour website at: Protected Critical Infrastructure Information (PCII) Program | CISA