NCCIC

National Cybersecurity and Communications Integration Center

PCII PROTECTIONS

What is PCII?

PCII is Protected Critical Infrastructure Information. As defined by the Critical Infrastructure Information Act of 2002, this type of information is described as "…information not customarily in the public domain and related to the security of critical infrastructure or protected systems."

To be eligible for protection, information must meet certain criteria. It must be

- voluntarily submitted,
- not customarily available in the public domain, and
- not submitted in lieu of compliance with any regulatory requirement.

Who Can Submit Information?

Asset owners of critical infrastructure or authorized representatives (e.g., security managers, legal counsel, or integrators on behalf of an asset owner) are able to submit information for consideration and protection.

How Does PCII Protect Information?

PCII protects validated data from

- Freedom of Information Act (FOIA) requests made of DHS (due to FOIA exemption "(b)3"),
- state, tribal, and local disclosure laws,
- use in regulatory actions, or
- use in civil litigations.

NOTE: Any reporting requirements imposed by a regulator are still applicable to the asset owner.

PCII protection means that asset owners partnering with DHS can be confident that sharing information with the government will not expose sensitive or proprietary data. Only trained and certified Federal, state, and local government employees or contractors may access PCII and only in accordance with strict safeguarding and handling requirements.

How Is PCII Data Protected?

The PCII Program Manager provides guidance to safeguard data and information to Authorized Users. PCII information sharing is only permitted between Authorized Users with a valid need-to-know for the limited purpose of assisting an asset owner.

To the extent feasible, submitted information is not at risk of inappropriate use. DHS will not disseminate PCII outside authorized channels.

How Easy Is It To Get PCII Protection?

An asset owner can request a PCII Express and Certification ("E&C") statement over the phone. Protections are in effect as soon as the asset owner returns the signed statement to NCCIC. All data, information, forensics, etc. associated with the incident are afforded all the protections described above.

Can PCII Protections be Set Up in Advance?

No. Because of the risk of changes to PCII protection statutes, processes, or responsible personnel, DHS is not able to support open-ended agreements of this nature.

What is Express PCII?

In certain circumstances, an asset owner may need to transmit critical proprietary information to NCCIC without time for the normal PCII submission and validation process. DHS considers this information as exigent PCII. Information received via this method can be given PCII protection immediately.

DHS will consider any information given over the phone or by secure email as protected while the Express and Certification statement is signed and returned to NCCIC.

About NCCIC

The National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.

http://www.dhs.gov/national-cybersecurity-communications-integration-center