PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCII) PROGRAM


PCII PROGRAM PROTECTIONS
Protects PCII from release through:
• Freedom of Information Act (FOIA) disclosure requests
• State, Local, Tribal or Territorial (SLTT) disclosure laws
• Use in civil litigation
• Use for regulatory purposes

PCII USES
Supports homeland security and its ability to understand and identify:
• Security risks and threats from physical and cyber-attack
• Vulnerabilities and mitigation strategies during special events
• Critical infrastructure security during planning and emergencies

AUTHORIZED USERS OF PCII
Federal, State, Local, Tribal or Territorial government employees and their designated contracted personnel are authorized access to PCII if they have:
• Completed PCII Authorized User training on the proper handling and safeguarding of PCII
• Homeland security duties and responsibilities
• A valid need-to-know
• Signed a non-disclosure agreement (non-Federal employees only)

SUBMITTERS OF PCII
Examples of organizations who submit CII for PCII protections are:
• Critical infrastructure owners and operators
• State, Local, Tribal or Territorial (SLTT) governments
• Collaborative homeland security working groups

QUALIFICATIONS FOR PCII PROTECTIONS
To qualify for PCII protections, information must be related to the security of the critical infrastructure and a submitter must attest the CII is:
• Voluntarily submitted
• Not customarily found in the public domain
• Not submitted in lieu of compliance with any regulatory requirement

CONTACT INFORMATION
To learn more about the PCII Program please visit us at www.dhs.gov/PCII or contact the PCII Program Office at PCII-Assist@hq.dhs.gov. PCII Program Help Desk Phone: 866-844-8163.