PCII PROGRAM OVERVIEW
The Protected Critical Infrastructure Information (PCII) Program, created by the U.S. Congress under the Critical Infrastructure Information Act of 2002 and implemented in 6 Code of Federal Regulations part 29, “Procedures for Handling Critical Infrastructure Information” encourages public and private sector owner(s) and operator(s) of physical and cyber critical infrastructure to voluntarily share sensitive security and proprietary information with CISA or other federal government agencies. The program supports the U.S. Government’s ability to understand and identify:
- Security risks and threats from physical and cyber-attacks
- Vulnerabilities, mitigation, and resilience strategies
- Critical infrastructure security during planning and emergencies

PCII PROGRAM PROVIDES LEGAL PROTECTION TO SENSITIVE INFORMATION
The PCII Program offers the following legal protections to private sector and state, local, tribal and territorial governments who voluntarily share critical infrastructure information, to include the submitter’s identity.

QUALIFICATIONS FOR PCII PROGRAM PROTECTIONS
Information must relate to the security of critical infrastructure and the submitter attests it is:
- Voluntarily submitted
- Not customarily found in the public domain
- Not submitted in lieu of compliance with any regulatory requirements

SUBMITTING CRITICAL INFRASTRUCTURE INFORMATION SECURELY IN 4 EASY STEPS
- Provide your information at https://pciims.cisa.gov/esubmission
- Complete Express and Certification Statements
- Drag documents to upload
- Select Submit
  The data is PROTECTED!

For additional PCII Program information and documents, please visit www.cisa.gov/pci
For program and technical issues, to include registration for training, please contact: TOC@mail.cisa.dhs.gov