



# Homeland Security

## IP Gateway

Our Nation's critical infrastructure is essential to the economy, security, and sustainment of the American way of life. The Department of Homeland Security (DHS) Office of Infrastructure Protection (IP) leads the coordinated national effort to protect critical infrastructure from all hazards by managing risk and enhancing resilience through collaboration with the critical infrastructure community.

Information systems play a vital role in allowing Federal, State, local, tribal, territorial, and private sector partners to identify, analyze, and manage risk to protect the Nation. The IP Gateway serves as the single interface through which DHS mission partners can access a large range of integrated IP tools and information to conduct comprehensive vulnerability assessments and risk analysis. This, in turn, enables homeland security partners to quickly identify relevant vulnerability and consequence data in support of event planning, incident preparedness, and response efforts.

### Features

The IP Gateway provides various data collection, analysis, and response tools in one integrated system, streamlining access to IP's tools and datasets by leveraging a single user registration, management, and authentication process. Highlights of the IP Gateway include the ability to access:

- A selection of physical and cyber vulnerability assessment and security surveys applications
- A consolidated library of critical infrastructure information, including assessments, analytical products, and reports
- Integrated data visualization and mapping applications to support complex data analysis
- Situational awareness applications to support special event and incident planning and response activities

### IP Gateway Administration & Access

The IP Gateway is available to State, local, tribal, and territorial governments to enhance collaboration in support of your respective infrastructure protection mission activities and to provide a mechanism for more streamlined cross-government information sharing. Each State, tribe, or territory interested in using the IP Gateway will be required to nominate an IP Gateway administrator, who will serve as the primary point of contact for the IP Gateway and will be responsible for vetting and granting access to other homeland security professionals. To obtain access to the IP Gateway, all users must be Protected Critical Infrastructure Information (PCII) certified and must complete required IP Gateway training.

### PCII Program

The Protected Critical Infrastructure Information (PCII) Program is an information-protection program that enhances voluntary information sharing between infrastructure owners and operators and the government. PCII protections mean that homeland security partners can be confident that sharing their information with the government will not expose sensitive or proprietary data.

### Contact Us

Learn how the IP Gateway can support your organization's homeland security efforts by contacting us at [IPGateway@hq.dhs.gov](mailto:IPGateway@hq.dhs.gov).