National Protection and Programs Directorate (NPPD)
Office of Infrastructure Protection (IP)

The Office of Infrastructure Protection (IP) leads the national effort to protect critical infrastructure from all hazards by managing risk and enhancing resilience through collaboration with the critical infrastructure community.

IP forges strong relationships with federal, state, local, tribal, and territorial government partners through the Protective Security Advisor (PSA) Program. Established by the Office of Infrastructure Protection (IP) in 2004, the PSA Program's primary mission is the protection of nationally significant critical infrastructure. In achieving this objective, Regional Directors and PSAs provide direct support to, and conduct crosscutting information sharing and coordination activities in support of, the following five mission areas:

- Plan, coordinate, and conduct security surveys and assessments;
- Plan and conduct outreach activities;
- Support National Special Security Events (NSSEs) and Special Event Activity Rating (SEAR) Level I and II events;
- Respond to incidents; and
- Coordinate and support improvised explosive device (IED) awareness and risk mitigation training.

The PSA Program maintains a robust operational field capability, strategically deploying 96 Regional Directors and PSAs—including 89 field-based personnel—to 73 districts in all 50 States and Puerto Rico. These personnel provide state, local, tribal, territorial, and private sector stakeholders with access to steady-state DHS risk-mitigation tools, products, and services (such as training and voluntary vulnerability assessments). PSAs also support response to all-hazard incidents through field-level coordination and information sharing, serving as Infrastructure Liaisons at Federal Emergency Management Agency Joint Field Offices; Regional Coordination Centers; and in State and county Emergency Operations Centers. By providing expert knowledge of affected infrastructure and maintaining communications with facility owner/operators, Regional Directors and PSAs help prioritize and coordinate critical infrastructure response, recovery, and restoration efforts.

PSAs engage with the United States Secret Service to provide critical infrastructure vulnerability assessments, security planning, and coordination during NSSEs and other large-scale special events (for instance, the Presidential Inauguration, the Super Bowl, and major international summits). PSAs also conduct joint site visits and vulnerability assessments with the Federal Bureau of Investigation.

Current IP Activities in the U.S. Insular Areas of Guam, American Samoa, Northern Mariana Islands, and U.S. Virgin Islands

Guam, American Samoa, & Northern Mariana Islands

Under the oversight of Federal Region IX Regional Director Frank Calvillo, Richard Mitchem (PSA - Hawaii District) supports IP field-based critical infrastructure protection activities within Hawaii, American Samoa, Guam, and the Northern Mariana Islands. PSA Mitchem has facilitated numerous infrastructure activities in American Samoa and Guam throughout 2013 with several more planned in 2014.

U.S. Virgin Islands

Under the oversight of Federal Region II Regional Director Frank Westfall, Julio Gonzalez-Rodriguez (PSA – Puerto Rico District) supports IP field-based critical infrastructure protection activities within Puerto Rico and the U.S. Virgin Islands. PSA Westfall has facilitated numerous infrastructure activities in the U.S. Virgin Islands throughout 2013 with several more planned in 2014.

Office of Infrastructure Protection Capabilities

Vulnerability Assessment and Security Survey Descriptions

- *Enhanced Critical Infrastructure Protection (ECIP) Security Surveys*

  By assessing the overall security posture of a facility, ECIP security surveys provide facility owner/operators with protective measures; information on facility importance and current terrorist threats; and develop strong relationships between critical infrastructure owner/operators, DHS, and Federal, State, and local law enforcement partners. During an ECIP visit, PSAs focus on coordination; outreach; training; and education, cataloguing existing relationships with Federal, State, local, and private sector partners. PSAs also discuss the Nationwide Suspicious Activity Reporting Initiative and the "If You See Something, Say Something"™ public awareness campaign with facility owner/operators.

  ECIP visits are often followed by ECIP security surveys to collect, process, and analyze facility assessment data and develop a detailed assessment of physical security, security management, security force, information sharing, protective measures, and dependencies to identify cascading effects. Data collected during ECIP surveys allows DHS and facility owner/operators to track the implementation of recommended protective measures; conduct sector-by-sector and cross-sector vulnerability comparisons; identify security gaps; provide owner/operators with a view of their facility's security in relation to similar facilities; and track progress toward improving critical infrastructure security. Infrastructure owner/operators are given security survey data in interactive ECIP Dashboards, enabling them to improve security postures in a cost-effective and measureable manner.

- *Computer Based Assessment Tool (CBAT) Imagery Captures*

  CBAT is a data collection and presentation medium designed to support critical infrastructure security, special event planning, and response operations. CBAT imagery captures provide immersive video, geospatial, and hypermedia data of critical facilities, surrounding areas, transportation routes, etc., and integrate assessment data from ECIP security surveys, Site Assistance Visits, and other relevant materials. Data is used to support the Regional Resiliency Assessment Program (RRAP); NSSEs and other special events; and the initiatives of facility owner/operators, local law enforcement, and emergency response personnel.

  The final CBAT product, a DVD containing self-executing presentation software, is provided to the facility representative, primary RRAP stakeholder, and/or special event security planning personnel, to facilitate security planning and in making rapid and informed incident preparedness and management decisions.

Office for Bombing Prevention (OBP) Counter-IED Risk Mitigation Training

OBP develops and delivers counter-IED risk mitigation training that builds knowledge among public and private sector partners regarding IED threats, incidents, associated implications, and counter-IED principles, policies, and programs that increase capability and capacity to detect, prevent, protect against, respond to, and mitigate IED threats.

- *IED Search Procedures Workshop*

  This workshop is designed to increase IED awareness and educate participants on bombing prevention measures and IED detection planning protocols by reviewing specific search techniques. The workshop builds knowledge of counter-IED principles and techniques among first responders and public/private sector security partners tasked with IED search and response protocols.

- *Bomb Threat Management Workshop*

  This workshop improves the ability of critical infrastructure owners, operators, and security personnel to manage IED threats by highlighting specific safety precautions associated with explosive incidents and bomb threats. The workshop reinforces an integrated approach that combines training, planning, and equipment acquisition to maximize available resources for bomb threat management. Public and private sector representatives knowledgeable in regional emergency management procedures are encouraged to attend.

- *IED Counterterrorism Workshop*

  This workshop enhances the participant’s understanding of the IED threat, surveillance detection methods, and soft target awareness. The workshop covers awareness and prevention measures as well as collaborative information-sharing resources to enable first responders and critical infrastructure owners, operators, and security staff in deterring, preventing, detecting, and protecting against the illicit and terrorist use of explosives in the United States.

Critical Infrastructure Community of Interest on the Homeland Security Information Network

The newly enhanced Critical Infrastructure Community of Interest on the Homeland Security Information Network (HSIN-CI) allows DHS and sector stakeholders to efficiently communicate, coordinate, and share information on a single platform. HSIN-CI serves as the primary vehicle for nationwide information sharing and collaboration between DHS, all 16 CI Sectors, and state and local fusion centers. In addition to providing tactical and planning functionality for vetted users, HSIN-CI is equipped with improved security measures to protect its libraries of over 60,000 publications, providing a network of trust to ensure the sustainability and integrity of service delivery and productivity of our Nation's Critical Infrastructure.

To gain access to HSIN-CI, please email your name, employer, work email address, and the CI Sector you are associated with to: hsinci@hq.dhs.gov.

The Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)

HITRAC generates incident specific Infrastructure Impact Assessments that include local infrastructure of concern and economic impacts.

National Critical Infrastructure Prioritization Program (NCIPP)

NCIPP is the identification and prioritization of critical infrastructure-the destruction or disruption of which could have catastrophic national or regional consequences-provides the foundation for infrastructure protection and risk reduction programs and activities executed by the Department of Homeland Security (DHS) and its public and private sector partners. DHS has historically executed this responsibility through an annual data call to sector, State, and territorial partners, using criteria developed by the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) National Critical Infrastructure Prioritization Program (NCIPP). The resulting list of critical infrastructure, prioritized in to two categories (Level 1 and Level 2), is used to inform the Department's infrastructure protection plans and programs to ensure that risk mitigation efforts are applied in the most effective way possible. The outcome of the NCIPP process is a critical infrastructure list for the territory used for situational awareness and strategic resource allocation.

Infrastructure of Concern (IOC)

HITRAC produces Infrastructure of Concern (IOC) Lists to identify critical infrastructure and key resources in response to changes in the infrastructure protection community's risk environment from terrorist attacks, natural hazards, and other events. The information is provided to support the activities of the Department, and to inform the strategies of Federal, State, local, and private sector partners designed to deter, prevent, preempt, and respond to terrorist attacks and other disruptions to infrastructure in the United States. The outcome of the IOC process is a prioritized list of infrastructure for significant federal response activities.