# Department of Homeland Security
# Office of Infrastructure Protection
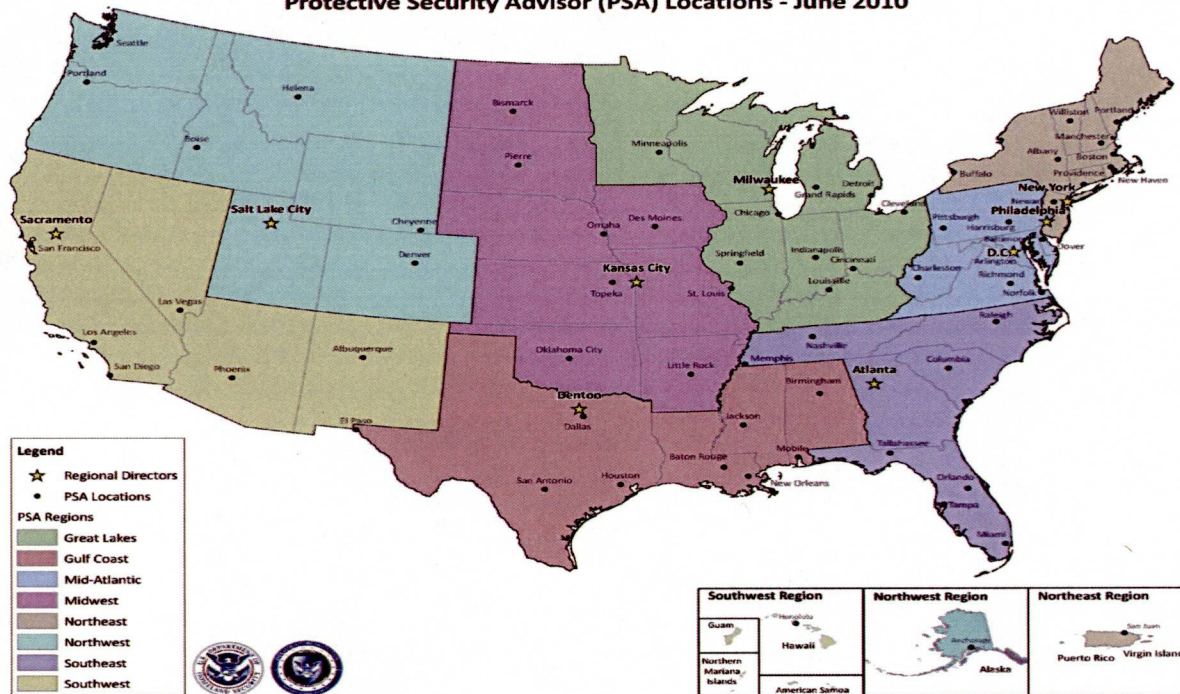
# Homeland Security

---

# Protective Security Advisors (PSAs)

- Cadre of 98 PSAs and Regional Directors serving local communities as critical infrastructure security specialists.
  - Average over 20 years of law enforcement, military, and anti-terrorism experience.

- Deployed to 70 Districts in 50 States and 1 Territory.

- Reside in the communities where they work.

- Fusion Center Partnership – DHS Intelligence Analyst Officers (IOs).

- State, local, tribal and territorial link to DHS infrastructure protection resources.
  - Coordinate vulnerability assessments, including Enhanced Critical Infrastructure Protection (ECIP)/Infrastructure Survey Tool (IST) assessments and training.
  - Provide support during incident management.
  - Provide vital link for information sharing.
  - Assist facility owners and operators with obtaining security clearances.

# PSA Locations



Protective Security Advisor (PSA) Locations - June 2010

# PSA Primary Responsibilities

- Assist with ongoing State and local CIKR security efforts coordinated by Homeland Security Advisors (HSAs).

- Support development of the national risk picture by identifying, assessing, monitoring, and minimizing risk to critical assets at the local and regional level.

- Assist with the implementation and execution of the National Infrastructure Protection Plan (NIPP).

- Upon request, facilitate and coordinate vulnerability assessments of local CIKR.

- Provide reach-back capability to DHS / NPPD.

- Advisory role – not regulatory or compliance driven

4

# Incident Management and Special Events

- Support response, recovery, and reconstitution efforts of States affected by a disaster.

  - Provide support in Joint Field Offices (JFOs).

  - Serve as pre-designated Infrastructure Liaison (IL) at the JFO when requested.

  - Help coordinate Federal, State, and local law enforcement CIKR protection efforts. Coordinate sharing of IP analysis within JFO.

  - Perform SAVs to identify vulnerabilities.

  - Provide advice on protective measures to enhance security at CIKR in and around impact area.

  - Provide key stakeholders with updates on issues relating to CIKR assets.

5

# Surveys, Assessments, Plans and Training

- Buffer Zone Protection Plans – fence line out, grants

- IST / ECIP – Infrastructure Survey Tool

- Site Assistance Visits (SAV's) – National Guard Bureau contract

- Data Call facilitation

- Soft Target Awareness Courses

- Bomb Surveys and Assessments

6

# Vulnerability Assessments - *PCII

## Site Assistance Visits (SAVs)

- Conducted in coordination and collaboration with other Federal, State, and local government entities, and critical infrastructure and key resources (CIKR) owners/operators.

- Conducted by NGB team (contracted by DHS) – PSA Fed Lead, Team Leader, Assault Planner, Systems Analyst

- Identifies CIKR dependencies, interdependencies, resiliency characteristics, and regional capability gaps.

- Increases owner/operator awareness of vulnerabilities and provides options for enhancing protective measures.

- Provides detailed reports to private sector partners used to make security enhancements.

## Buffer Zone Protection Program (BZPP)

- An infrastructure protection grant program targeted to first responders and managed jointly by FEMA Grant Programs Directorate and DHS IP.

- Seeks to build terrorism prevention and protection capabilities in States and local communities through allowable planning and equipment acquisition by local law enforcement and first responders.

- Supports the development of effective preventive/protective measures that make it more difficult for terrorists to conduct surveillance or launch attacks from the immediate vicinity of CIKR.

> *Protected Critical Infrastructure Information – Federal Law CIA 2002

# Cyber Resiliency Review (CRR)

- Conducted by DHS team from the National Cyber Security Division (NCSD)

- Evaluate how CIKR organizations manage the cybersecurity of significant information services and assets (information, technology, resources, and personnel)

- Identify opportunities for improvement in cyber security management and reduce operational risks related to cybersecurity

- Information protected by PCII – FOIA, State Disclosure Laws, Civil Litigation.

# Computer-Based Assessment Tool (CBAT)

- A computer-based visual cross-platform tool to capture critical site assets and current security postures.

- Integrates SAV and Buffer Zone Plan (BZP) assessment data with geospherical video and geospatial and hypermedia data.

- Assists owners/operators, local law enforcement, and emergency response personnel, to prepare for, respond to, and manage CIKR, National Special Security Events (NSSEs), high-level special events, and contingency operations.

# Regional Resiliency Assessment Program (RRAP)

- Reduces the Nation's vulnerability to natural and manmade threats by evaluating CIKR on a regional level and coordinating protection efforts to enhance resiliency and the security of the surrounding communities and geographic regions.

- The RRAP is an interagency assessment of selected CIKR and regional analysis of the surrounding infrastructure that:
  - Examines vulnerabilities, threats, and potential consequences from an all-hazards perspective using enhanced assessment methodology.
  - Identifies CIKR dependencies, interdependencies, resiliency characteristics, and gaps.
  - Evaluates the prevention and protection capabilities of owners/operators, local law enforcement, and emergency response organizations.
  - Provides baseline examination of risk and metrics to measure mitigation.
  - Coordinates and integrates program execution.

# Enhanced Critical Infrastructure Protection (ECIP) Initiative

- ECIP assessments conducted to:
  - Identify and recommend protective measures at facilities, provide comparison across like assets, and track implementation of new protective measures.
  - Inform facility owners and operators of the importance of their facilities as an identified high-priority infrastructure and the need to be vigilant.
  - Discuss NPPD/IP programs.
  - Establish/enhance relationships with facility owners and operators.
  - Conducted in conjunction with the Infrastructure Survey Tool (IST).

11

# Infrastructure Survey Tool (IST)

- Web-based vulnerability assessment tool that applies weighted scores to identify vulnerabilities and trends for infrastructure and across sectors.

- Facilitates the consistent collection of vulnerability assessment information.

- The IST will allow DHS to:
  - Identify and document trends in infrastructure strengths and weaknesses.
  - Provide information for protective measures planning and resource allocation.
  - Enhance overall capabilities, methodologies, and resource materials for identifying and mitigating vulnerabilities.
  - Facilitate government information sharing.

12

# Protective Security Coordination Division

- Office for Bombing Prevention (OBP)
  - DHS' lead for bombing prevention activities
  - Seeks to reduce the Nation's risk to terrorist bombing attacks using tools such as TRIPwire and TRIPwire Community Gateway, National Capabilities Analysis Database (NCAD), Multi-Jurisdiction Improvised Explosive Device Security Plans (MJIEDSPs), and the National IED Awareness Campaign.

- Vulnerability Assessments Branch (VAB)
  - Conducts vulnerability assessments in partnership with Federal, State, local, and private sector security partners to prevent, deter, and mitigate the risk of a terrorist attack while enabling timely response and restoration in all-hazards situations.

- Field Operations Branch (FOB)
  - Deployed Protective Security Advisors (PSAs) to all 50 States and 1 Territory to serve as a Federal resource to communities and businesses, assist in the protection of U.S. critical infrastructure and key resources (CIKR), and further State and local homeland security initiatives.

13

# Department of Homeland Security Office of Infrastructure Protection

Don Ronsberg, Protective Security Advisor
North Dakota District
U.S. Dept of Homeland Security
Mobile: 701-516-3940      Office: 701-250-4429      Fax: 701-250-4430
Federal Bldg
304 E. Broadway, Suite 219
Bismarck ND 58501

US Department of Homeland Security Website:
http://www.dhs.gov/index.shtm

US DHS Critical Infrastructure Information:
http://www.dhs.gov/files/programs/critical.shtm

Homeland
Security