Infrastructure Security Division

Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

Protective Security Coordination Division

Protective Security Advisor Program and Services

3/28/2019
Protective Security Advisors

- PSAs are non-regulatory, field-deployed personnel who serve as critical infrastructure security and resilience advisors
- Link State, local, tribal, and territorial (SLTT) and private sector partners to DHS resources and services
  - Coordinate vulnerability assessments, training, and other DHS products and services
  - Share information in steady state, during special events and incidents
  - Assist facility owners and operators with obtaining security clearances
- During contingency events, PSAs support the response, recovery, and reconstitution efforts
  - Man state and local emergency operations centers
  - Serve as pre-designated Infrastructure Liaisons (IL) at Joint Field Offices
## Protective Security Advisor Locations

**Protective Security Advisor (PSA) Locations - December 11, 2018**

### Region I

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
<th>Title</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>John Doe</td>
<td>New York</td>
<td>PSA</td>
<td>NY</td>
</tr>
<tr>
<td>Jane Smith</td>
<td>Boston</td>
<td>PSA</td>
<td>MA</td>
</tr>
</tbody>
</table>

### Region II

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
<th>Title</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robert Jones</td>
<td>Chicago</td>
<td>PSA</td>
<td>IL</td>
</tr>
<tr>
<td>Mary Wilson</td>
<td>Dallas</td>
<td>PSA</td>
<td>TX</td>
</tr>
</tbody>
</table>

### Region III

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
<th>Title</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sarah Lee</td>
<td>Miami</td>
<td>PSA</td>
<td>FL</td>
</tr>
<tr>
<td>David Martinez</td>
<td>Houston</td>
<td>PSA</td>
<td>TX</td>
</tr>
</tbody>
</table>

### Region IV

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
<th>Title</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lisa Brown</td>
<td>Los Angeles</td>
<td>PSA</td>
<td>CA</td>
</tr>
<tr>
<td>Tom Jackson</td>
<td>Denver</td>
<td>PSA</td>
<td>CO</td>
</tr>
</tbody>
</table>

### Region V

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
<th>Title</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emily Davis</td>
<td>Seattle</td>
<td>PSA</td>
<td>WA</td>
</tr>
<tr>
<td>Michael Wilson</td>
<td>Portland</td>
<td>PSA</td>
<td>OR</td>
</tr>
</tbody>
</table>

### Region VI

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
<th>Title</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Olivia Green</td>
<td>New Orleans</td>
<td>PSA</td>
<td>LA</td>
</tr>
<tr>
<td>Rachel White</td>
<td>Orlando</td>
<td>PSA</td>
<td>FL</td>
</tr>
</tbody>
</table>

### Region VII

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
<th>Title</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simon Black</td>
<td>San Antonio</td>
<td>PSA</td>
<td>TX</td>
</tr>
<tr>
<td>Emily Johnson</td>
<td>Austin</td>
<td>PSA</td>
<td>TX</td>
</tr>
</tbody>
</table>

### Region VIII

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
<th>Title</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>David Martinez</td>
<td>Phoenix</td>
<td>PSA</td>
<td>AZ</td>
</tr>
<tr>
<td>Lisa Brown</td>
<td>Las Vegas</td>
<td>PSA</td>
<td>NV</td>
</tr>
</tbody>
</table>

### Region IX

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
<th>Title</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sarah Lee</td>
<td>Honolulu</td>
<td>PSA</td>
<td>HI</td>
</tr>
<tr>
<td>Robert Jones</td>
<td>San Juan</td>
<td>PSA</td>
<td>PR</td>
</tr>
</tbody>
</table>
Protected Critical Infrastructure Information

- Established under the Critical Infrastructure Information Act of 2002
- Protects voluntarily submitted critical infrastructure information from:
  - Freedom of Information Act
  - State and local sunshine laws
  - Civil litigation proceedings
  - Regulatory usage
- Provides private sector with legal protections and “peace of mind.”
Site Assistance Visit

- Establishes and enhances DHS’s relationship with critical infrastructure owners and operators

- During a Site Assistance Visit (SAV) visit, PSAs focus on coordination, outreach, training, and education

- SAV visits include local, state, and federal response and support partners to enable everyone to gain a better understanding of the site and enable us all to move forward together

- Perfect one stop shop to meet the local players of importance
Infrastructure Survey Tool

- The IST is a web-based vulnerability survey tool that applies weighted scores to identify infrastructure vulnerabilities and trends across sectors

- Collects data for a snapshot in time for sites for feedback

- The Dashboard tool allows facility owners and operators to:
  - Compare a facility’s security in relation to similar facilities
  - Identify security gaps
  - Track progress toward improving critical infrastructure security
Example Dashboard - Protection

Overview of PMI

INSTRUCTIONS: To view the details of any component on the chart below, click on the corresponding blue bars. To view the responses used to calculate the PII, click on the side navigation menu options.

Compared to: 144 (Office Building - Stand Alone)
Assessment Finalized Date: April 12, 2012
Refresh Date: February 09, 2018
Tracking Number: PCI1234

WARNING: Data contained on this system is Protected Critical Infrastructure Information. Link to more info
Active Shooter: Preparation and Response Presentations

- Based on 2012 Joint DHS/FBI Bulletin and best practices
- Background Information on personalities that perpetrate these attacks
  - Propensity towards violence, mental illness, triggering point
  - To aid employees and disrupt possible events
- Planning
  - Individual mental maps
  - Organizational plans
- Response – Situationally based: Run, Hide or Fight
- Recovery – based on plans and profound nature of attack
- Additional resources
Western PA/PA Region 13 Task Force
Utility Subcommittee Meetings

- Have EMA and Utility Co-Chairs to guide discussion/direction
- Quarterly meetings at various times and locations
- All major western PA Utility Companies invited
- Have looked at resilience and restoration procedures
  - Government and utility
- Visited sites to see how they depend on utility services
- Back to interactions between 911 Centers/EMAs and Utilities
Counter-IED Training & Awareness

- Diverse curriculum of training designed to build counter-IED core capabilities, such as:
  - IED Counterterrorism Workshop
  - Surveillance Detection
  - Bomb Threat Management
  - Vehicle-Borne IED (VBIED) Search
  - Protective Measures
  - IED Search Procedures

- Increases knowledge and ability to detect, prevent, protect against, and respond to bombing threats

Courtesy of DHS OBP
PSA Initiatives
See Something Say Something

• Adopted by the Commonwealth in 2016
• Nationwide Suspicious Activity Reporting Initiative (NSI)
• State has canned information and posters available through the Governor’s Office of Homeland Security
• DHS support in preparation of material, posters, etc
• Pittsburgh Cultural District role model
Homeland Security Information Network (HSIN)

- HSIN (https://hsin.dhs.gov/) is DHS’s primary technology tool for trusted information sharing

- HSIN – Critical Infrastructure (HSIN-CI) enables direct communication between:
  - DHS
  - Federal, State, and local governments
  - Critical infrastructure owners and operators

- Content includes:
  - Planning and Preparedness
  - Incident Reporting and Updates
  - Situational Awareness
  - Education and Training
Increase awareness of the infrastructure mission and build a baseline of security and resilience knowledge throughout the Nation

Identify Common Vulnerabilities, Potential Indicators of Terrorist Activity, and associated Protective Measures, along with actions that can be undertaken to enhance resilience

Courtesy of DHS
DHS/IP - Partners

Domestic Security Office
Pennsylvania State Police

What is RVAT?
RVAT is comprised of a group of Pennsylvania State Troopers who are highly trained in conducting professional risk and vulnerability assessments.

What is a Risk and Vulnerability Assessment?
A risk and vulnerability assessment is a comprehensive examination of physical facilities and operational procedures. The assessment will identify critical assets, the threat potential, and vulnerabilities. The assessment will also include recommendations to improve the security posture of the facility.

What areas will be assessed?
The assessment will focus on a multitude of areas, including: parking, access control, closed circuit TV systems, lighting, mail handling, HVAC systems, emergency preparedness, employee screening, and other security related areas.

How long does an assessment take?
The length of the assessment depends on the size of the facility. Generally, a comprehensive assessment lasts between one and three days.

What is the role of the requestor?
The requestor will be asked to provide copies of emergency procedures, floor plans, and security policies. Assessors may also interact with employees and ask questions regarding security matters.

How are the results presented?
At the conclusion of the assessment, the assessor(s) will provide a verbal overview of findings to the requestor. A comprehensive written report will be subsequently prepared and provided.

What type of facility qualifies for an assessment?
Virtually any type of facility, public or private, qualifies for an assessment. For multi-tenant structures, it is important that the building manager or owner cooperates during the assessment process.

How much does the assessment cost?
ALL PSP RVAT ASSESSMENTS ARE FREE OF CHARGE.

How do I schedule a risk & vulnerability assessment?
Contact the RVAT at 717-346-4085/717-346-2654 or by e-mail: ra-pspoffdomesticsecurity@pa.gov

ra-pspoffdomesticsecurity@pa.gov
PA Fusion Centers

- The Pennsylvania Criminal Intelligence Center (PaCIC)
- The Pennsylvania State Police (PSP) information sharing between criminal justice agencies and critical infrastructure owners and operators
- Complete registration form designating your Sector
- sp-protectPA@pa.gov or 855-772-7768
- Western PA All Hazards Fusion Center – wpahfc@pa.gov
DHS/IP – Partners

- An information-sharing and analysis effort serving the interests and combining the knowledge of a wide range of members
- Partnership between FBI and private sector
- Businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent/mitigate acts against the United States
- http://www.infragard.net
Private Sector Resources Catalog

- www.dhs.gov/private-sector-resources-catalog
- All DHS agencies have available material
- Training
  - FEMA, Active Shooter, Workplace Violence, Surveillance Detection
- Information
  - Homeland Security Information Network, TripWire, National Terrorism Alert System, National Suspicious Activity Reporting
- Services
  - Wireless Priority Service (WPS)/Government Emergency Telephone System (GETS), Geographic Information Systems
- Systems
  - Protected Critical Infrastructure Information, Chemical Facility Anti-Terrorism Standards, Business Continuity
- Cyber – Assessments, bulletins, and best practices
DHS Cyber Security Programs

- **Cyber Resilience Review (CRR)**
  - Evaluate how CIKR providers manage cyber security of significant information services and assets

- **Cyber Infrastructure Survey Tool (C-IST)**
  - Identify and document critical cyber security information including system-level configurations and functions, cyber security threats, cyber security measures, IT business continuity/disaster recovery and cyber security organizational management

- **Cyber Security Evaluation Tool (CSET)**
  - Self-assessment using recognized standards
  - [http://us-cert.gov/control_systems/csetdownload.html](http://us-cert.gov/control_systems/csetdownload.html)
DHS Cyber Security Programs - CSET

- Network Mapping
- System comparisons to chosen standards
- Hard copy reports
- Resource library
## Cyber Security Contact Information

### Evaluation Inquiries

<table>
<thead>
<tr>
<th>Email Address</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:cse@hq.dhs.gov">cse@hq.dhs.gov</a></td>
</tr>
</tbody>
</table>

### CSA Program

<table>
<thead>
<tr>
<th>Email Address</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:cyberadvisor@hq.dhs.gov">cyberadvisor@hq.dhs.gov</a></td>
</tr>
<tr>
<td><a href="mailto:Franco.cappa@hq.dhs.gov">Franco.cappa@hq.dhs.gov</a></td>
</tr>
</tbody>
</table>

---

Department of Homeland Security  
Cybersecurity and Infrastructure Security Agency  
Office of Cybersecurity and Communications
For more information, visit: www.dhs.gov/critical-infrastructure

Bob Winters - bob.winters@dhs.gov
Protective Security Advisor - Pittsburgh