The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

Protective Security Advisor Overview

Southwest Section AWWA Conference & Exposition

October 2016
Role of DHS

- Unify a national effort to secure America
- Prevent and deter terrorist attacks
- Protect against and respond to threats and hazards to the Nation
- Respond to and recover from acts of terrorism, natural disaster, or other emergencies
- Coordinate the protection of our Nation’s critical infrastructure across all sectors
Threats May Come from All Hazards

Courtesy of FEMA
Critical Infrastructure Defined

“Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.”

Source: National Infrastructure Protection Plan 2013

Courtesy of FEMA
Critical Infrastructure Sectors

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities

- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems

Courtesy of DHS
Security and Resilience Challenges

- A majority of critical infrastructure is privately owned
- DHS has limited legal authority to regulate security practices of private industry
  - Exceptions: National Protection and Programs Directorate Office of Infrastructure Protection (high-risk chemicals), Transportation Security Administration, and United States Coast Guard
- DHS; Sector-Specific Agencies; other Federal entities; the private sector; and State, local, tribal, and territorial governments all have roles and responsibilities in critical infrastructure protection
Operational Mission Areas

- Conduct Security Surveys, Gap Analysis, and Assessments
- Conduct Outreach Activities
- Support National Special Security Events (NSSEs) and Special Event Activity Rating (SEAR) Events
- Respond to Incidents
- Provide Improvised Explosive Device (IED) Awareness & Risk Mitigation Training
Protective Security Advisors

- PSAs are field-deployed personnel who serve as critical infrastructure security specialists
  - Regional Directors (RDs) oversee and manage the PSA program in their respective region
- State, local, tribal, and territorial (SLTT) and private sector link to DHS infrastructure protection resources
  - Coordinate vulnerability assessments, training, and other DHS products and services
  - Provide a vital link for information sharing in steady state and incident response
  - Assist facility owners and operators with obtaining security clearances
- During contingency events, PSAs support the response, recovery, and reconstitution efforts of the States by serving as pre-designated Infrastructure Liaisons (IL) and Deputy ILs at the Joint Field Offices
Protective Security Advisor Locations

Protective Security Advisor (PSA) Locations - July 21, 2015

Courtesy of DHS
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.”

Courtesy of DHS
Examples of Critical Infrastructure Information

- Protected information defined by the Critical Infrastructure Information Act includes:
  - Threats – Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of a critical asset
  - Vulnerabilities – Ability to resist threats, including assessments or estimates of vulnerability
  - Operational experience – Any past operational problem or planned or past solution including repair, recovery, or extent of incapacitation

- Any information normally available in the public domain will not be protected
Enhanced Critical Infrastructure Protection Visit

- Establishes and enhances DHS’s relationship with critical infrastructure owners and operators, informs them of the importance of their facilities, and reinforces the need for continued vigilance.

- During an Enhanced Critical Infrastructure Protection (ECIP) visit, PSAs focus on coordination, outreach, training, and education.

- ECIP visits are often followed by security surveys using the Infrastructure Survey Tool (IST) or Rapid Survey Tool (RST), or delivery of other IP services.
Infrastructure Survey Tool

- The IST is a web-based vulnerability survey tool that applies weighted scores to identify infrastructure vulnerabilities and trends across sectors
- Facilitates the consistent collection of security information
  - Physical Security
  - Security Force
  - Security Management
  - Information Sharing
  - Protective Measures
  - Dependencies
Infrastructure Survey Tool (cont.)

- Generates the Protective Measures Index and Resilience Measurement Index

- The tool allows DHS and facility owners and operators to:
  - Identify security gaps
  - Compare a facility’s security in relation to similar facilities
  - Track progress toward improving critical infrastructure security
The Dashboards highlight areas of potential concern and feature options to view the impact of potential enhancements to protection and resilience measure.

The written report, developed from the IST data, contains a description of the facility and its vulnerabilities as well as recommendations to mitigate identified vulnerabilities.
IST Survey Data Categories

- Facility Information
- Contacts
- Facility Overview
- Information Sharing*
- Protective Measures Assessment*
- Criticality*
- Security Management Profile*
- Security Areas/Assets
- Additional DHS Products/Services
- Criticality Appendix
- Images

- Security Force*
- Physical Security*
  - Building Envelope
  - Delivery/Vehicle Access Control
  - Parking
  - Site’s Security Force
  - Intrusion Detection System (IDS)/Close Circuit Television (CCTV)
  - Access Control
  - Security Lighting
- Cyber Vulnerability
- Dependencies*

* Comparative analysis provided
Dashboards and Information Sharing

Greater understanding of the most significant changes and trends.

Areas individually separated into Physical Security, Security Management, Security Force, Information Sharing, and Protective Measures. Owner/Operator can make adjustments and see improvements to individual area and overall Protective Measure Index (PMI).
Dashboard – Physical Security Example

Notional Information
Infrastructure Visualization Program

- Infrastructure Visualization Program ((IVP))
  - A data collection and presentation medium that supports critical infrastructure security, special event planning, and response operations by leveraging assessment data and other relevant materials
  - Integrates assessment data with immersive video, geospatial, and hypermedia data
  - Assists facility owners and operators, local law enforcement, and emergency response personnel to prepare for, respond to, and manage critical infrastructure, National Special Security Events (NSSEs), high-level special events, and contingency operations
Infrastructure Visualization Program (cont.)
The Regional Resiliency Assessment Program (RRAP) began in 2009 as a pilot program out of efforts to assess security of individual critical assets.

The goal is to identify opportunities for regional homeland security officials and critical infrastructure partners to strengthen resilience to all hazards.

The RRAP process identifies critical infrastructure security and resilience gaps; dependencies; interdependencies; cascading effects; and State, local, tribal, and territorial government capability gaps.
Regional Resiliency Assessment Program (cont.)

- The RRAP process identifies critical infrastructure security, resilience, dependencies, interdependencies, cascading effects, and State, local, tribal, and territorial agency capability gaps

- Conducted 57 RRAP projects from Fiscal Year (FY) 2009 through FY 2015
  - Diverse and dynamic set of critical infrastructure topics, sectors, and regions
Active Shooter Training and Outreach Materials

- DHS materials consist of three products:
  - Basic Guide Book.
  - Pocket Emergency Measures Guide.
  - Break Room Poster.

- To download these materials visit:
  - [www.dhs.gov/activeshooter](http://www.dhs.gov/activeshooter)
Homeland Security Starts with Hometown Security

Security starts here.

connect  plan  train  report

Homeland Security
Protective measures for public gatherings

- Soft targets/public gathering places are attractive targets for our adversaries
- Americans congregate daily to work, play, shop, learn, celebrate, worship, and watch sports and entertainment at a variety of locations:
  - Concert halls and theatres
  - Restaurants and shopping malls
  - Parades and fairs
  - Houses of worship
  - Sports venues
- Our adversaries may perceive locations like these as attractive targets
Counter-IED Training & Awareness

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

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

Courtesy of DHS OBP
Counter-IED Training & Awareness

Bomb-Making Materials Awareness Program (BMAP)

- Joint DHS-FBI program that promotes private sector point-of-sale awareness and suspicious activity reporting to prevent misuse of dual-use explosive precursor chemicals and components commonly used in IEDs
- Increases prevention opportunities by building a network of aware and vigilant private sector partners

Courtesy of DHS/FBI
TRIPwire
Technical Resource for Incident Prevention

- Secure information sharing platform for IED incident information, evolving IED tactics, lessons learned, and counter-IED preparedness information
- Builds knowledge and preparedness capabilities, filling vital gaps in information sharing

Courtesy of TRIPwire
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
InfraGard

- [https://www.infragard.org](https://www.infragard.org)

InfraGard is an information-sharing and analysis effort serving the interests of and combining the knowledge base of a wide range of members.

At its most basic level, InfraGard is a partnership between the Federal Bureau of Investigation (FBI) and the private sector.

InfraGard is an association of businesses, academic institutions, State and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States.
Infrastructure Protection Report Series

- 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 Cyber Security Evaluations

<table>
<thead>
<tr>
<th>Name</th>
<th>Cyber Resilience Review (CRR)</th>
<th>Cyber Infrastructure Survey Tool (C-IST)</th>
<th>Supply Chain Risk Management Review</th>
<th>Onsite Cyber Security Evaluation Tool (CSET) Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>Identify cyber security management capabilities and maturity</td>
<td>To calculate a comparative analysis and valuation of protective measures in-place</td>
<td>Identify external dependencies and the risks associated</td>
<td>Provides a detailed, effective, and repeatable methodology for assessing control systems security – while encompassing an organization’s infrastructure, policies, and procedures.</td>
</tr>
<tr>
<td><strong>Scope</strong></td>
<td>Critical Service view</td>
<td>Critical Cyber Service view</td>
<td>Organization / Business Unit</td>
<td>Industrial Control Systems</td>
</tr>
<tr>
<td><strong>Time to Execute</strong></td>
<td>5 to 6 Hours</td>
<td>2 ½ to 4 Hours</td>
<td>2 to 2 ½ Hours</td>
<td>8 Hours (1 Business Day)</td>
</tr>
<tr>
<td><strong>Information Sought</strong></td>
<td>Capabilities and maturity indicators in 10 security domains</td>
<td>Protective measures in-place</td>
<td>Third-party security requirements and contract management info</td>
<td>Industrial control system’s core functions, infrastructure, policies, and procedures</td>
</tr>
<tr>
<td><strong>Preparation</strong></td>
<td>Short, 1-hour questionnaire plus planning call(s)</td>
<td>Planning call to scope evaluation</td>
<td>Planning call to scope evaluation</td>
<td>Coordinated via Email. Planning call(s) if requested.</td>
</tr>
<tr>
<td><strong>Participants</strong></td>
<td>IT/Security Manager, Continuity Planner, and Incident Responders</td>
<td>IT/Security Manager</td>
<td>IT / Security Manager with Contract Management</td>
<td>control system operators/engineers, IT, policy/management personnel, and subject matter experts.</td>
</tr>
</tbody>
</table>
# DHS Cyber Security Evaluations

<table>
<thead>
<tr>
<th>Name</th>
<th>ICS-CERT Design Architecture Review (DAR)</th>
<th>ICS Network Architecture Verification and Validation (NAVV)</th>
<th>Network Risk and Vulnerability Assessment (RVA)</th>
<th>Cyber Hygiene (CH) Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Supports the cybersecurity design via investigative analysis, production, and maintenance of control systems and ICS components.</td>
<td>Provides analysis and base-lining of ICS communication flows, based upon a passive (non-intrusive) collection of TCP Header Data.</td>
<td>Perform penetration and deep technical analysis of enterprise IT systems and an organization’s external resistance to specific IT risks</td>
<td>Identify public-facing Internet security risks, at a high-level, through service enumeration and vulnerability scanning</td>
</tr>
<tr>
<td>Scope</td>
<td>Industrial Control Systems/Network Architecture</td>
<td>Industrial Control Systems/Network Architecture/Network Traffic</td>
<td>Organization / Business Unit / Network-Based IT Service</td>
<td>Public-Facing, Network-Based IT Service</td>
</tr>
<tr>
<td>Time to Execute</td>
<td>2 Days (8 Hours Each Day)</td>
<td>Variable (Hours to Days)</td>
<td>Variable (Days to Weeks)</td>
<td>Variable (Hours to Continuous)</td>
</tr>
<tr>
<td>Information Sought</td>
<td>Network design, configurations, interdependencies, and its applications.</td>
<td>Network traffic header-data to be analyzed with Sophia Tool.</td>
<td>Low-level options and recommendations for improving IT network and system security</td>
<td>High-level network service and vulnerability information</td>
</tr>
<tr>
<td>Preparation</td>
<td>Coordinated via Email. Planning call(s).</td>
<td>Coordinated via Email. Planning call(s).</td>
<td>Formal rules of engagement and extensive pre-planning</td>
<td>Formal rules of engagement and extensive pre-planning</td>
</tr>
<tr>
<td>Participants</td>
<td>Control system operators/ engineers, IT personnel, and ICS network, architecture, and topologies SMEs</td>
<td>Control system operators/ engineers, IT personnel, and ICS network, architecture, and topologies SMEs</td>
<td>IT/Security Manager and Network Administrators</td>
<td>IT/Security Manager and Network Administrators</td>
</tr>
</tbody>
</table>
Summary

- Facilitate local field activities in coordination with other DHS offices
- Provide partners with effective vulnerability and gap analyses, bombing prevention capability analyses, and the development of protective measures to identify emerging needs and areas for investment
- Through data collection, assessment, and analysis, DHS can generate products for Federal, State, and local officials and private sector owners and operators that drive initiatives, such as infrastructure protection grant programs and research and development requirements
How Can You Help?

- Engage with PSAs and other partners on critical infrastructure protection programs and initiatives
- Encourage participation in efforts to identify, assess, and secure critical infrastructure in your community
- Communicate local concerns related to critical infrastructure protection
- Enhanced security and resilience depends on developing and strengthening partnerships between all entities with a role in critical infrastructure protection
For more information, visit:
www.dhs.gov/critical-infrastructure

Chad Johnston
Protective Security Advisor - AR
Chad.Johnston@hq.dhs.gov