The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

Protective Security Coordination Division Overview

Name of Stakeholder

Date of Briefing

Homeland Security

PSA 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

Homeland Security

Protective Security Advisor Locations

Courtesy of DHS

Homeland Security

PSA Tools

Site Assistance 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 a Site Assistance Visit (SAV), PSAs focus on coordination, outreach, training, and education
- SAVs are often followed by security surveys using the Infrastructure Survey Tool (IST) or delivery of other IP services

Homeland Security

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

Homeland Security

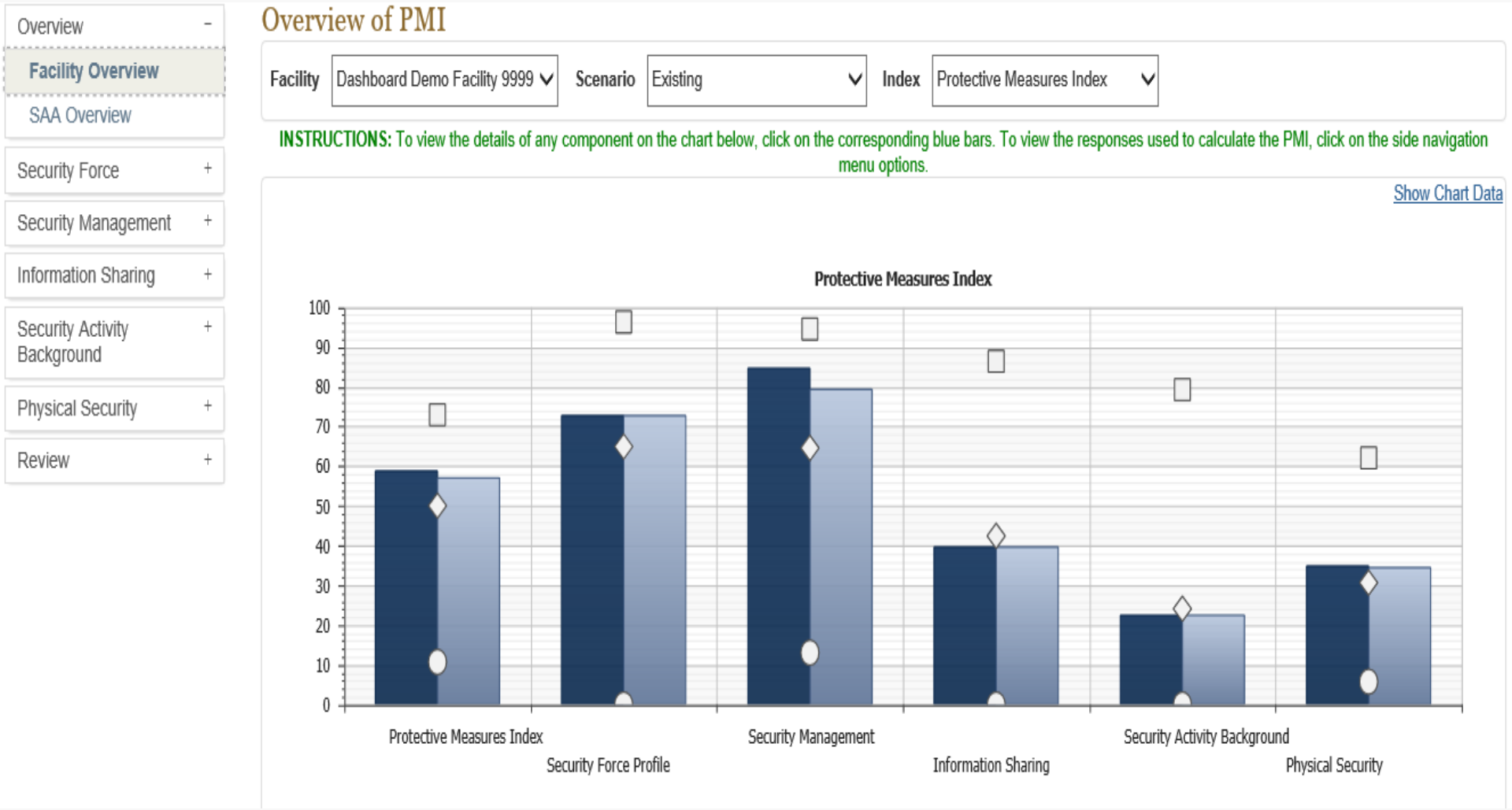
IST Deliverables

Table 2 Facility and SAA Vulnerabilities and Options for Consideration

	Category	Vulnerability	Option(s) for Consideration
	Security Management Profile	The facility's security plan is missing key elements.	Update the security plan to include the following: • Illumination[3] • Security force staffing[4] • Security force training[5] • Access control procedures for contractors • A security awareness training program that addresses internal disturbances (e.g., workplace violence) – Develop a protocol to respond to workplace violence. Refer to the Federal Bureau of Investigation (FBI) Website for resources, such as the January 2011 *FBI Law Enforcement Bulletin: Workplace Violence Prevention*, available at http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/january2011/january_2011. – Include policies and procedures to respond to workplace violence threats and incidents in the security plan. – Provide training on workplace violence to all personnel at initial hire and annually thereafter. • A security awareness training program that addresses security communications policy or procedures • A security awareness training program that addresses information protection/operation security • A security awareness training program that addresses hostage situations • Liaison with response agencies • Exercising the plan • Plan maintenance (e.g., review and revision)
	Security Management Profile	Background checks are not conducted on contractors.	• Require contracting companies to conduct background checks on their personnel who will work at the facility and to make such records available for audit.[6]

Homeland Security

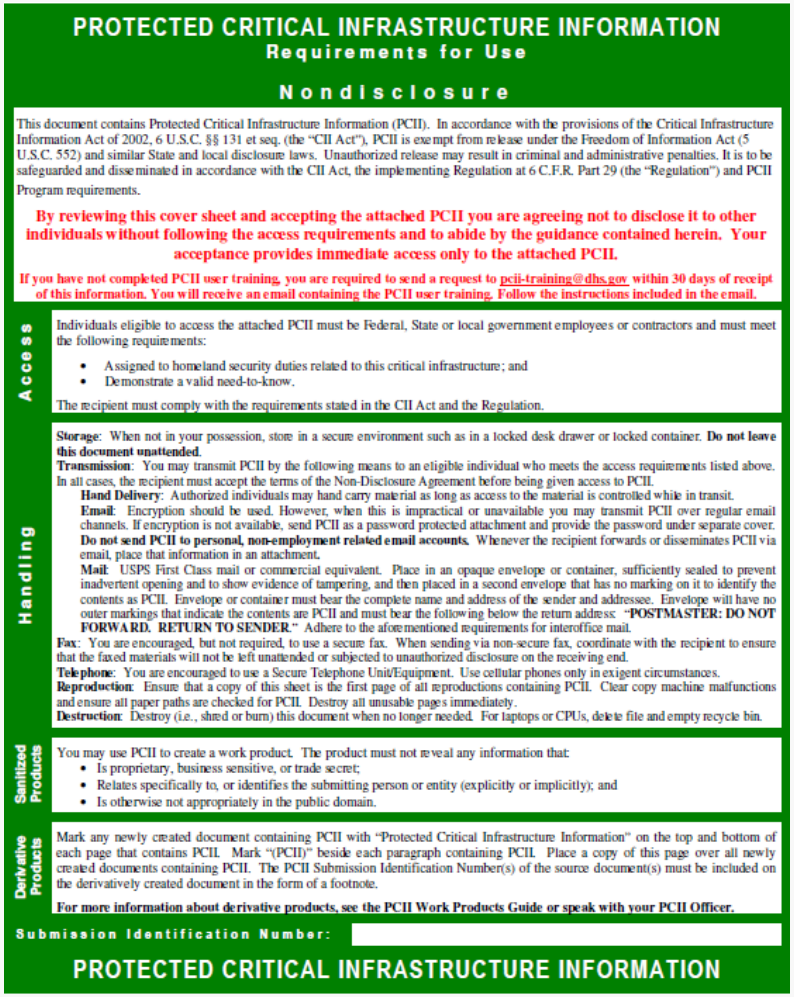
IST Deliverables



Homeland Security

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.”



PROTECTED CRITICAL INFRASTRUCTURE INFORMATION
Requirements for Use

Nondisclosure

This document contains Protected Critical Infrastructure Information (PCII). In accordance with the provisions of the Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 131 et seq. (the “CII Act”), PCII is exempt from release under the Freedom of Information Act (5 U.S.C. 552) and similar State and local disclosure laws. Unauthorized release may result in criminal and administrative penalties. It is to be safeguarded and disseminated in accordance with the CII Act, the implementing Regulation at 6 C.F.R. Part 29 (the “Regulation”) and PCII Program requirements.

By reviewing this cover sheet and accepting the attached PCII you are agreeing not to disclose it to other individuals without following the access requirements and to abide by the guidance contained herein. Your acceptance provides immediate access only to the attached PCII.

If you have not completed PCII user training, you are required to send a request to pcii-training@dhs.gov within 30 days of receipt of this information. You will receive an email containing the PCII user training. Follow the instructions included in the email.

Access

Individuals eligible to access the attached PCII must be Federal, State or local government employees or contractors and must meet the following requirements:

- Assigned to homeland security duties related to this critical infrastructure; and
- Demonstrate a valid need-to-know.

The recipient must comply with the requirements stated in the CII Act and the Regulation.

Handling

Storage: When not in your possession, store in a secure environment such as in a locked desk drawer or locked container. **Do not leave this document unattended.**
Transmission: You may transmit PCII by the following means to an eligible individual who meets the access requirements listed above. In all cases, the recipient must accept the terms of the Non-Disclosure Agreement before being given access to PCII.
Hand Delivery: Authorized individuals may hand carry material as long as access to the material is controlled while in transit.
Email: Encryption should be used. However, when this is impractical or unavailable you may transmit PCII over regular email channels. If encryption is not available, send PCII as a password protected attachment and provide the password under separate cover. **Do not send PCII to personal, non-employment related email accounts.** Whenever the recipient forwards or disseminates PCII via email, place that information in an attachment.
Mail: USPS First Class mail or commercial equivalent. Place in an opaque envelope or container, sufficiently sealed to prevent inadvertent opening and to show evidence of tampering, and then placed in a second envelope that has no marking on it to identify the contents as PCII. Envelope or container must bear the complete name and address of the sender and addressee. Envelope will have no outer markings that indicate the contents are PCII and must bear the following below the return address: **“POSTMASTER: DO NOT FORWARD. RETURN TO SENDER.”** Adhere to the aforementioned requirements for interoffice mail.
Fax: You are encouraged, but not required, to use a secure fax. When sending via non-secure fax, coordinate with the recipient to ensure that the faxed materials will not be left unattended or subjected to unauthorized disclosure on the receiving end.
Telephone: You are encouraged to use a Secure Telephone Unit/Equipment. Use cellular phones only in exigent circumstances.
Reproduction: Ensure that a copy of this sheet is the first page of all reproductions containing PCII. Clear copy machine malfunctions and ensure all paper paths are checked for PCII. Destroy all unusable pages immediately.
Destruction: Destroy (i.e., shred or burn) this document when no longer needed. For laptops or CPUs, delete file and empty recycle bin.

Sanitized Products

You may use PCII to create a work product. The product must not reveal any information that:

- Is proprietary, business sensitive, or trade secret;
- Relates specifically to, or identifies the submitting person or entity (explicitly or implicitly); and
- Is otherwise not appropriately in the public domain.

Derivative Products

Mark any newly created document containing PCII with “Protected Critical Infrastructure Information” on the top and bottom of each page that contains PCII. Mark “(PCII)” beside each paragraph containing PCII. Place a copy of this page over all newly created documents containing PCII. The PCII Submission Identification Number(s) of the source document(s) must be included on the derivatively created document in the form of a footnote.

For more information about derivative products, see the PCII Work Products Guide or speak with your PCII Officer.

Submission Identification Number:

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

Courtesy of DHS

Homeland Security

Infrastructure Visualization Platform

- Infrastructure Visualization Platform (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

Active Shooter Preparedness Briefs

- DHS aims to enhance preparedness through a “whole community” approach by providing training products, and resources to a broad range of stakeholders on issues such as active shooter awareness, incident response, and workplace violence. In many cases there is no pattern or method to selection of victims by an active shooter, and these situations are, by their very nature, unpredictable and evolve quickly. DHS offers free courses, materials, and workshops to better prepare you to deal with an active shooter situation and to raise awareness of behaviors that represent pre-incident indicators and characteristics of active shooters.

Homeland Security

Infrastructure Protection Report Series

Courtesy of DHS

- 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

Homeland Security

Counter-IED Training & Awareness

Courtesy of DHS OBP

- 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

Homeland Security

TRIP*wire*

Technical Resource for Incident Prevention

Courtesy of TRIPwire

- 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

Homeland Security

Other Products and Services (cont.)

Bomb Threat Guidance and Vehicle Inspection Guide

Courtesy of DHS OBP

- Bomb Threat Guidance provides a quick-reference for managing in-progress bomb threats for schools, businesses, and government facilities with information on police coordination, threat assessment, search, and evacuation versus shelter-in-place considerations
- Vehicle Inspection Guide assists Government and private sector security personnel in conducting vehicle inspection operations to prevent vehicle-borne IEDs

Homeland Security

Cyber Support for Critical Infrastructure

- National Cybersecurity and Communications Integration Center (NCCIC)
  - United States Computer Emergency Readiness Team (US-CERT) Operations Center
  - Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Operations Center
  - National Cybersecurity Assessment & Technical Services (NCATS)
- US-CERT
- Control Systems Security Program
- Cyber Exercise Program
- Cyber Security Evaluations Program
- Cyber Security Advisors

Homeland Security

Homeland Security

For more information, visit:
www.dhs.gov/critical-infrastructure

Kyle Wolf

Protective Security Advisor

Kyle.wolf@hq.dhs.gov

Homeland Security