The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

PSCD 101 Overview Brief

Water ISAC

April 15, 2014

Homeland Security

Vision and Mission

- Vision - A safe, secure, and resilient critical infrastructure based on, and sustained through, strong public and private partnerships
- Mission - Lead the National effort to mitigate terrorism risk to, strengthen the protection of, and enhance the all-hazard resilience of the Nation's critical infrastructure

Homeland Security

The Role of Homeland Security

- 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

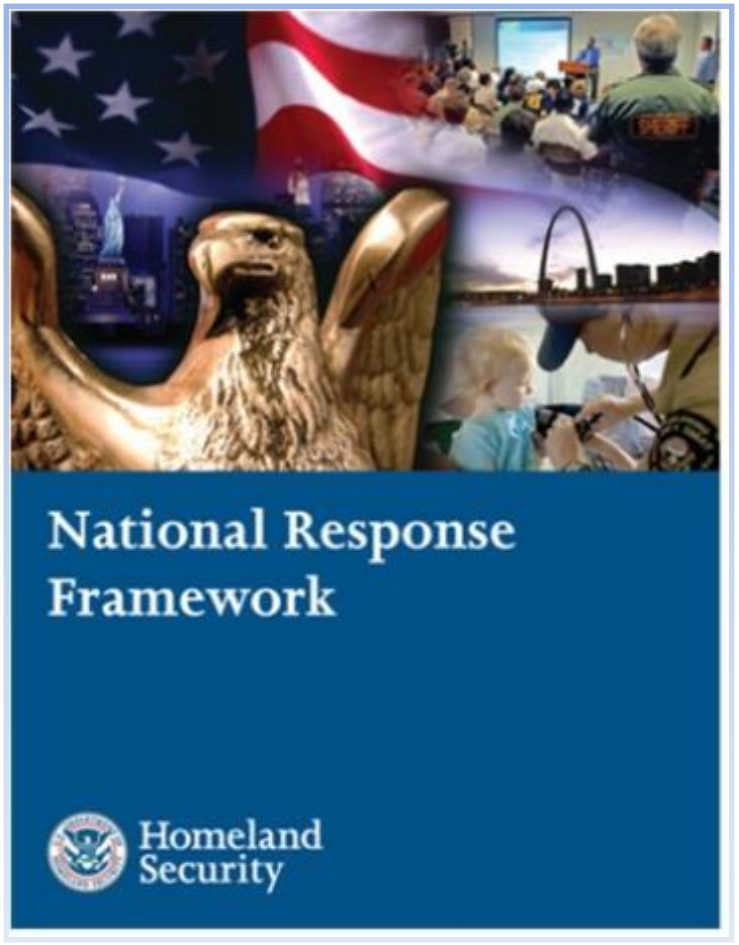
Homeland Security

Threats May Come from All Hazards

Homeland Security

National Response Framework

- Guides how the Nation conducts all-hazards response
- Documents the key response principles, roles, and structures that organize national response
- Allows first responders, decisionmakers, and supporting entities to provide a unified national response



Homeland Security

Presidential Policy Directive-21

- Announced in February 2013, *Presidential Policy Directive-21: Critical Infrastructure Security and Resilience* replaces Homeland Security Presidential Directive-7 and directs the Executive Branch to:
  - Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time
  - Understand the cascading consequences of infrastructure failures
  - Evaluate and mature the public-private partnership
  - Update the National Infrastructure Protection Plan
  - Develop comprehensive research and development plan

Critical Infrastructure Defined

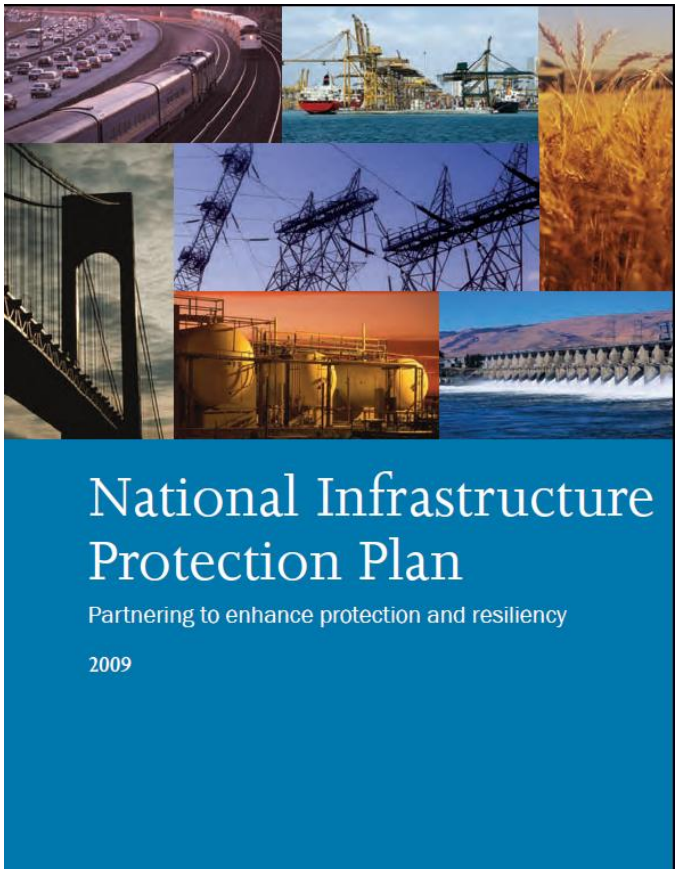
- Critical Infrastructure
  - "Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional,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

  Source: National Infrastructure Protection Plan 2009

Homeland Security

National Infrastructure Protection Plan

- Comprehensive plan and unifying structure for the public and private sector to enhance the protection and resilience of critical infrastructure
  - Partnership model
  - Risk management framework
  - Roles, responsibilities, and authorities
- Drives internal programs and activities, and guides those of:
  - Other Federal agencies and departments
  - State, local, tribal, and territorial governments
  - Critical infrastructure owners and operators



Homeland Security

Critical Infrastructure Sectors

- Banking and Finance
- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water

Homeland Security

Critical Infrastructure Protection Challenges

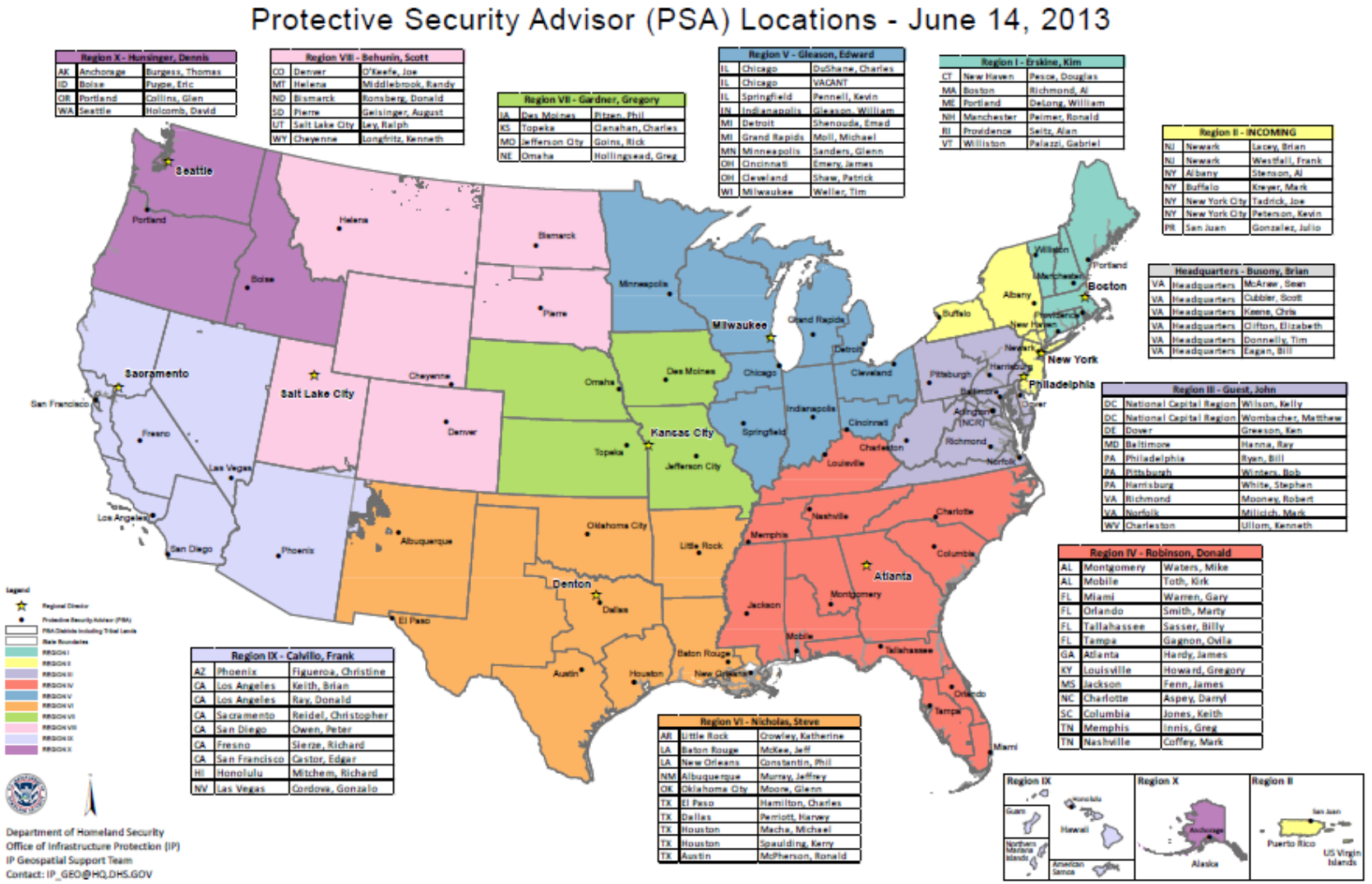
- A majority of critical infrastructure privately-owned
- The Department of Homeland Security (DHS) has limited legal authority to regulate security practices of private industry (exceptions: National Protection and Programs Directorate Office of Infrastructure Protection (high-risk chemicals), Transportation Security Administration, 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

Protective Security Advisors

- 96 PSAs and Regional Directors, including 89 field deployed personnel, serve as critical infrastructure security specialists
- Deployed to 73 Districts in 50 states and Puerto Rico
- State, local, tribal, territorial, 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

Homeland Security

Protective Security Advisor Locations



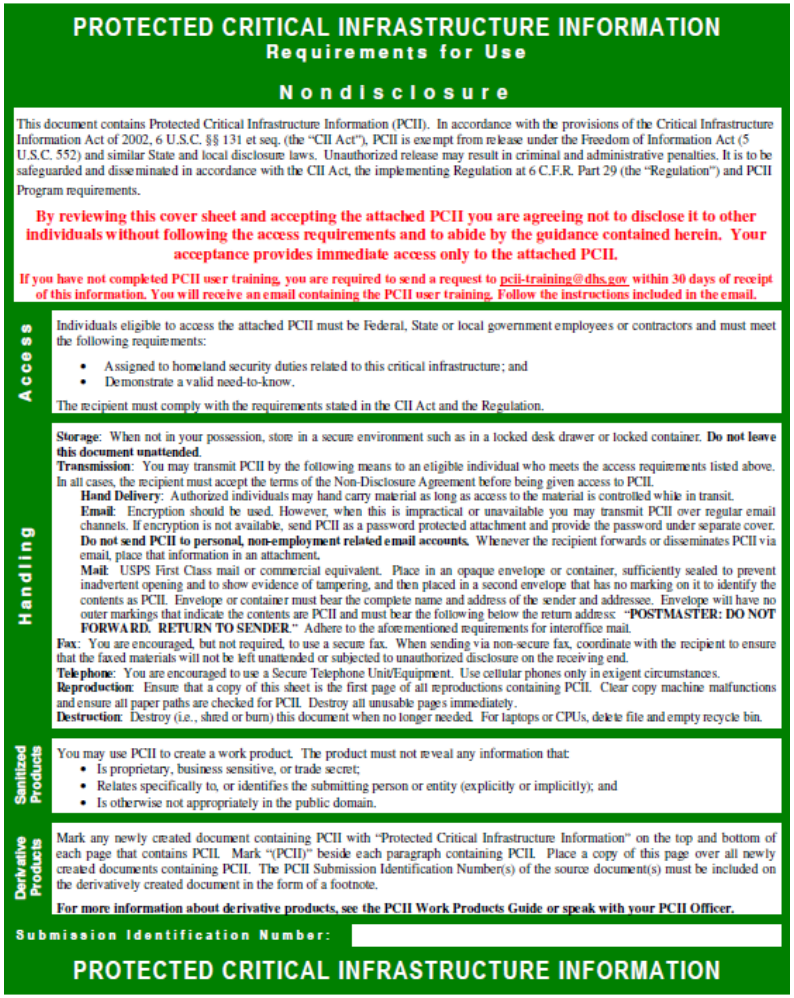
Homeland Security

Value of the PSA Program

- PSAs:
  - Support comprehensive risk analyses for critical infrastructure
  - Assist in the review and analysis of physical/technical security for critical infrastructure
  - Convey local concerns and sensitivities to DHS and other Federal agencies
  - Relay disconnects between local, regional, and National protection activities
  - Communicate requests for Federal training and exercises

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

Homeland Security

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, of incapacitation of a critical asset
  - Vulnerabilities – Ability to resist threats, including assessments or estimated 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

Homeland Security

Enhanced Critical Infrastructure Protection Initiative

- Establishes/enhances DHS relationship with facility owners and operators, and informs owners and operators of the importance of their facilities and the need to be vigilant
- ECIP survey
  - Identifies facilities' physical security, security forces, security management, protective measures, information sharing, and dependencies
  - Tracks implementation of new protective measures
- ECIP Dashboard
  - Creates facility protective measures index that can be used to compare against similar facilities
  - Tool for informing protective measures planning and resource allocation
- Information is protected under the PCII program
- Information used by DHS for steady-state analysis and incident management

Homeland Security

ECIP Survey Tool

- Web-based vulnerability survey tool that applies weighted scores to identify vulnerabilities and trends for infrastructure and across sectors
- Facilitates the consistent collection of security information
  - Physical Security, Security Force, Security Management, Information Sharing, Protective Measures, Dependencies
- The tool allows DHS to:
  - Identify and document critical infrastructure overall security
  - Provide information for protective measures planning and resources allocation
  - Facilitate government information sharing
  - Enhance its ability to analyze data and produce improved metrics

Homeland Security

ECIP 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
  - IDS/CCTV
  - Access Control
  - Security Lighting
- Cyber Vulnerability
- Dependencies*

* Comparative analysis provided

Homeland Security

Weighting Process and Participants

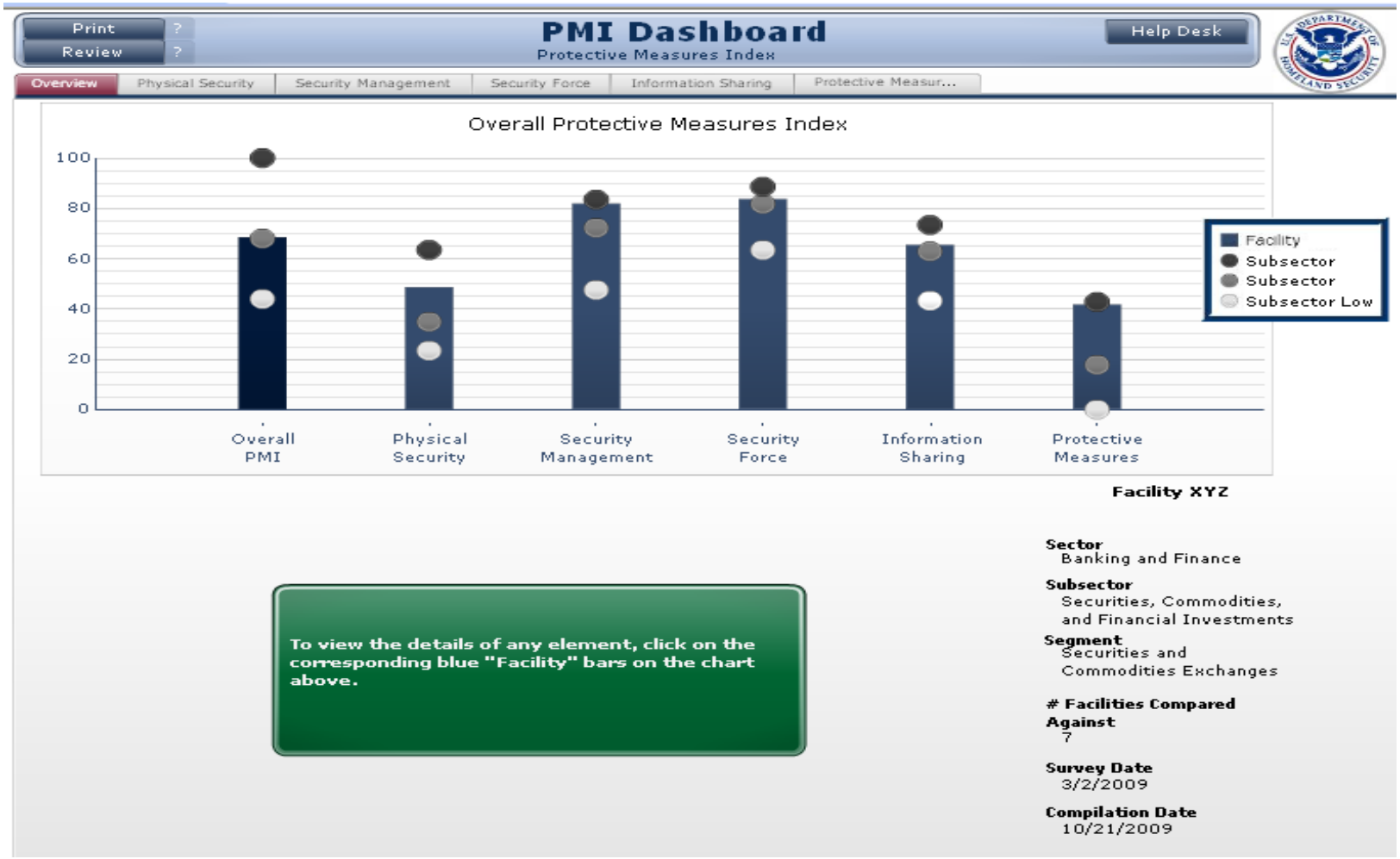
- Scoring for Physical Security, Security Management, and Security Force was conducted using a working group comprised of:
  - Physical security experts
  - Scientists
  - Mathematicians
  - Sector representatives
  - Owners and operators of facilities being weighted
- Weights validated using a separate panel of representatives
- Example: Fences

- Aluminum chain link fence
- 7 foot height
- With outriggers
- Barbed wire
- Fence Protective Measures Index = 71

- Wood fence
- 6 foot height
- Partial clear zone
- Fence Protective Measures Index = 13

Homeland Security

ECIP Deliverables

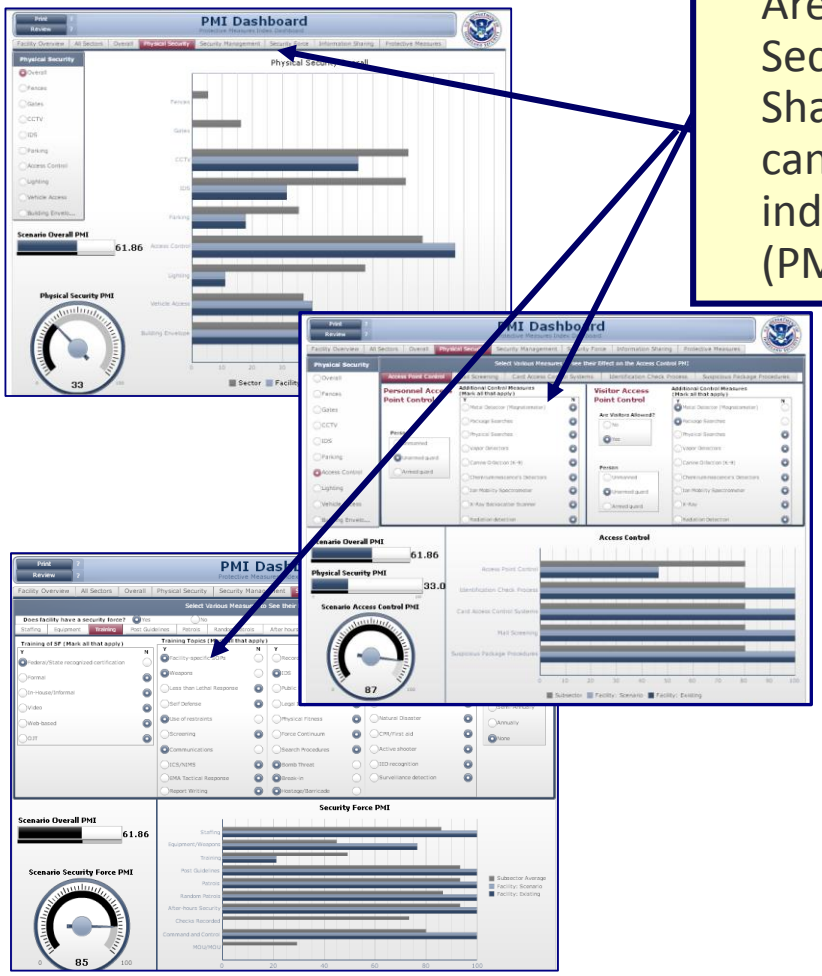


Notional Information

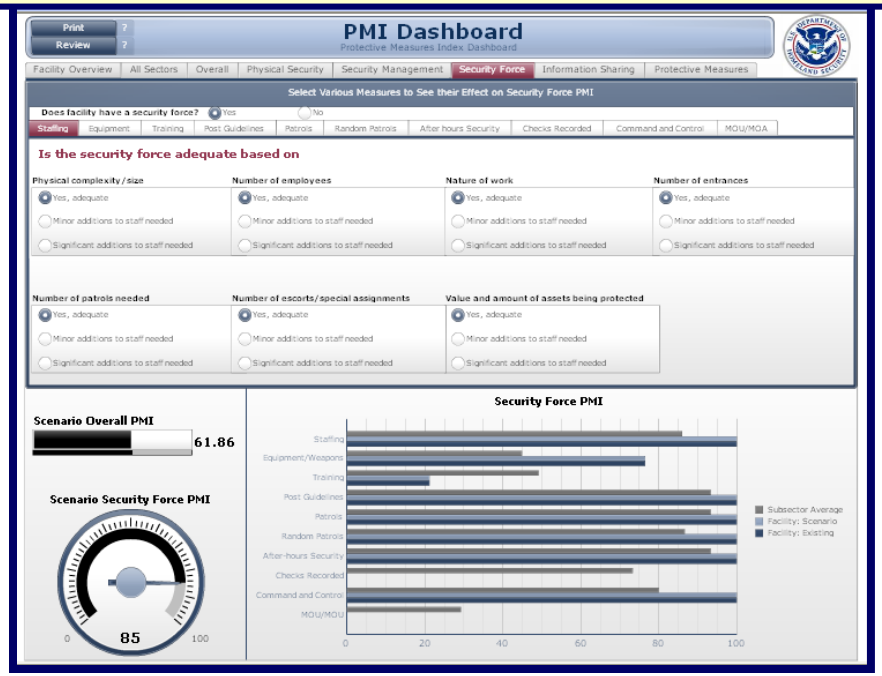
Homeland Security

Dashboards and Information Sharing

Owner / Operator Protective Measure Index Dashboard



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).

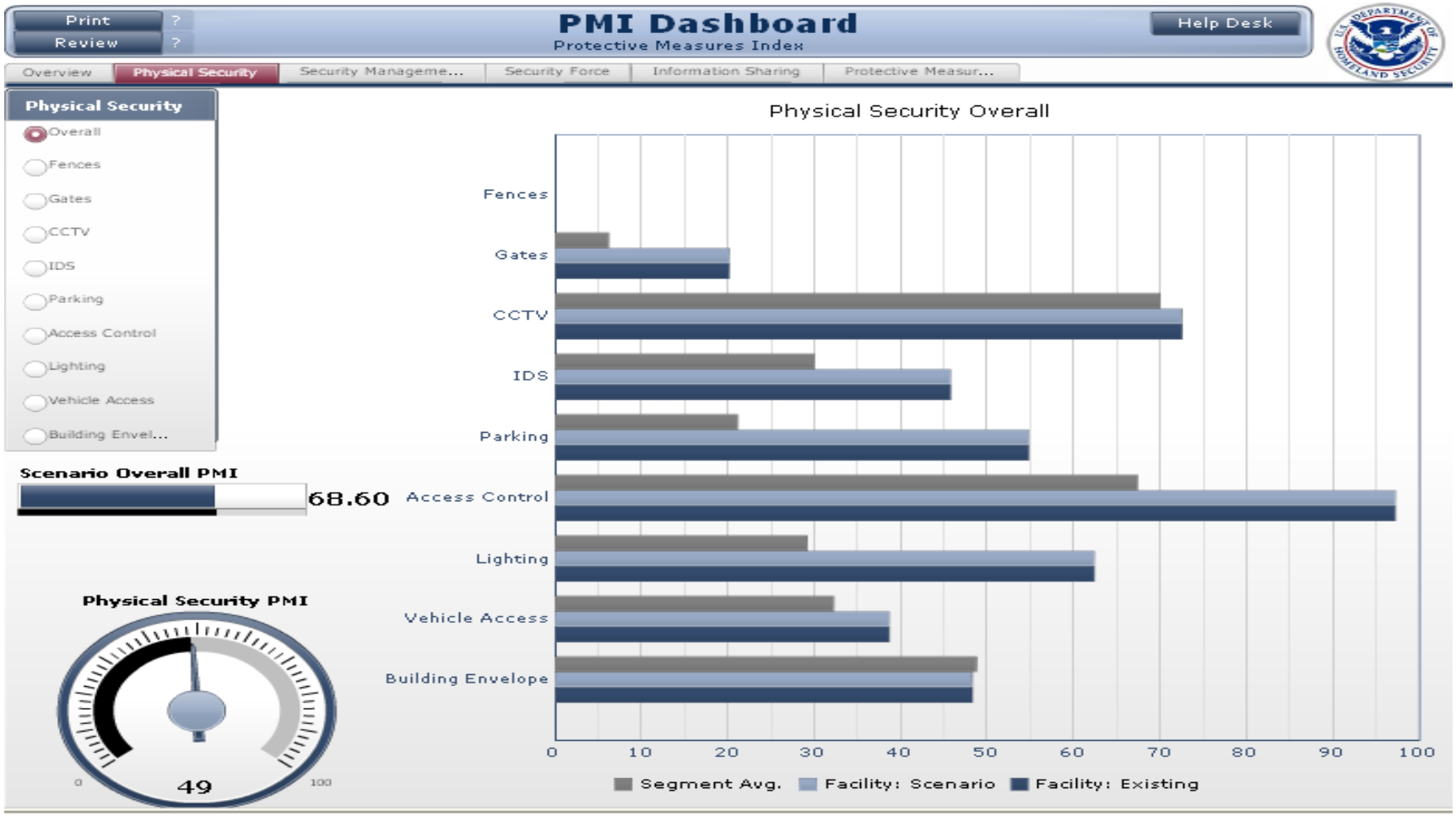


Greater understanding of the most significant changes and trends.

* *Information provided is notional ECIP survey information and does not contain real survey information*

Notional Information

Dashboard – Physical Security Example

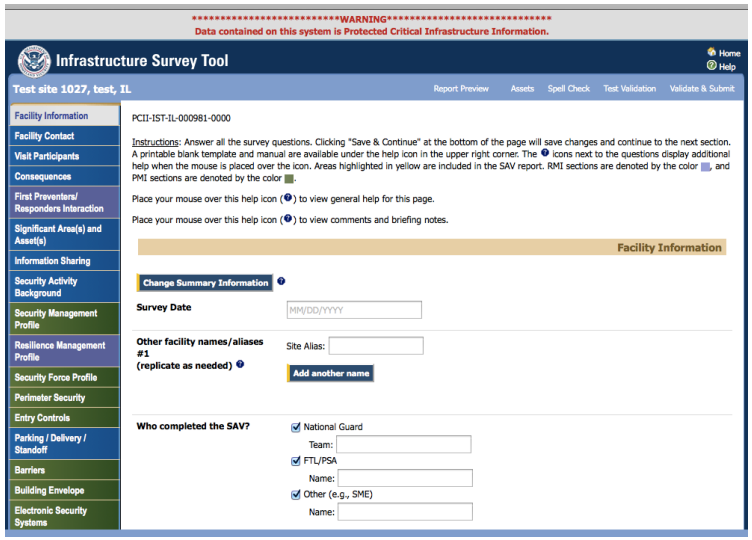


Homeland Security

Notional Information

Infrastructure Survey Tool

- New version roll-out on January 8, 2013
- Web-Based Tool
  - New tabs
  - Same “buttonology”
  - Still can have an Access Builder
- Major Changes
  - Physical Security is almost the same and generates the Protective Measures Index (PMI)
  - More on resilience and business continuity to generate the new Resilience Measurement Index (RMI)
  - Natural hazard mitigation is more detailed
  - Dependencies questions incorporate RRAP-Only tab questions



Other Products and Resources

- DHS InfraGard
- DHS Homeland Security Information Network (HSIN)
- DHS Vulnerability Assessments
- DHS Infrastructure Protection Report Series
- DHS Bomb-making Materials Awareness Program
- DHS TRIPwire and Security Training

InfraGard

- http://www.infragard.net
- InfraGard is an information-sharing and analysis effort serving the interests 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 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

Homeland Security Information Network

- HSIN is DHS's primary technology tool for trusted information sharing
- HSIN – Critical Sectors (HSIN-CS) enables direct communication between DHS; Federal, State, and local governments; and infrastructure owners and operators
- Content Includes:
  - Planning and Preparedness: Risk assessments, analysis, guidance, and security products; geospatial products and hurricane models; exercise and national event info
  - Incident Reporting and Updates: Real-time situational reports and alerts
  - Situational Awareness: Daily and monthly sector-specific and cross-sector reports on topics ranging from cybersecurity to emerging threats
  - Education and Training: Training on topics ranging from critical infrastructure resilience, to threat detection and reaction for retail staff

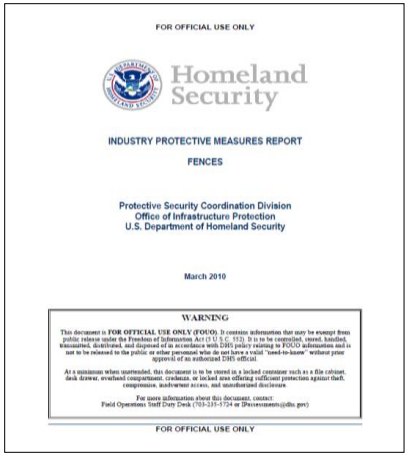
Homeland Security

Vulnerability Assessment Programs

- Site Assistance Visits
  - Brings together Federal, State, and local partners and owners and operators to conduct an “inside the fence” assessment that identifies significant assets, vulnerabilities, protective measures, critical dependencies, and options for improving security and resilience. The findings are compiled in a final product that is PCII-protected
- Computer Based Assessment Tool
  - A computer-based visual cross-platform tool that displays critical site assets and current security postures
  - Integrates assessment data with immersive video, geospatial, and hypermedia data
  - Assists owners and operators, local law enforcement, and emergency response personnel, to prepare for, respond to, and manage critical infrastructure, National Special Security Events, high-level special events, and contingency operations

Homeland Security

Infrastructure Protection Report Series


FOR OFFICIAL USE ONLY

Homeland Security

INDUSTRY PROTECTIVE MEASURES REPORT

FENCES

Protective Security Coordination Division
Office of Infrastructure Protection
U.S. Department of Homeland Security

March 2010

WARNING

This document is **FOR OFFICIAL USE ONLY (FOUO)**. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

At a minimum when unattended, this document is to be stored in a locked container such as a file cabinet, desk drawer, overhead compartment, credenza, or locked area offering sufficient protection against theft, compromise, inadvertent access, and unauthorized disclosure.

For more information about this document, contact:
Field Operations Staff Duty Desk (703-235-3724 or IPassessments@dhs.gov)

FOR OFFICIAL USE ONLY


FOR OFFICIAL USE ONLY

U.S. Department of Homeland Security
Protective Security Coordination Division
Office of Infrastructure Protection

Infrastructure Protection Report Series

Natural Gas Storage

The approximately 400 natural gas underground storage (UGS) facilities located throughout the United States are critical to maintaining the reliability, integrity, and market-response capability of the Nation's natural gas transmission and distribution network. The most common type of UGS facilities are (1) depleted reservoirs in oil and/or gas fields, (2) aquifers, (3) caverns (formations), (4) domed mines, and (5) hard rock cavities (see figure below).

Potential Indicators of Terrorist Activity

Terrorists have a wide variety of weapons and tactics available to achieve their objectives. Specific threats of most concern to UGS systems include:

- Improvised explosive devices (IEDs)
- Vehicle-borne improvised explosive devices (VBIEDs)
- Sabotage
- Cyber attack
- Electromagnetic pulse (EMP) attack

Terrorist activity indicators are observable anomalies or incidents that may precede a terrorist attack. Indicators of an imminent attack requiring immediate action may include the following:

- Vehicles approaching or lingering near the facility, wellhead, or its security boundary in a suspicious or threatening manner
- Suspicious or illegally-parked vehicles near facilities, wellheads, or other sensitive areas
- A suspicious package in a sensitive area that might contain explosives
- Persons or teams of people spotted in or around the site attempting to gain unauthorized access to restricted areas
- Persons appearing to prepare to launch standoff weapons (e.g., rocket-propelled grenades) at the facility
- Persons walking through open fields near wellhead facilities
- Recent damage to a perimeter fence or gate, perimeter lighting, security cameras, motion sensors, or other security devices
- Recent vandalism associated with critical structural or mechanical parts of the facility

Indicators of potential surveillance by terrorists include:

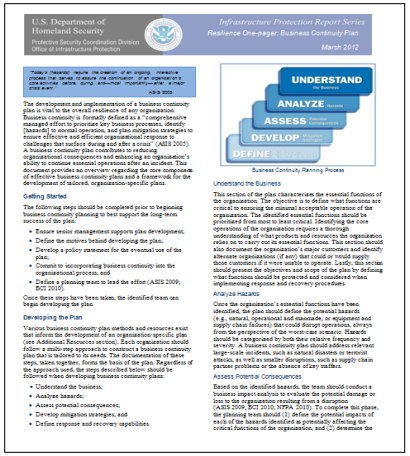
- Persons possessing or using observation equipment (e.g., cameras, binoculars, night-vision devices) near the facility over an extended period
- Persons discovered with maps, photos, or diagrams with facilities or key facility components highlighted
- Persons parking, standing, or loitering in the same area over an extended period with no reasonable explanation
- Employees whose working behavior has changed or who are working more irregular hours without explanation
- Persons questioning employees off-site about practices pertaining to UGS facility operations or security measures
- Persons questioning utility or communications company employees about the site's supporting systems
- Unfamiliar service or contract personnel with passable credentials attempting to access unauthorized areas

Common Vulnerabilities

The following are key common vulnerabilities of UGS facilities:

- Presence on-site of large quantities of flammable and explosive materials
- Remote locations far from emergency responders
- Difficulty of perimeter control due to nature of facilities and assets
- Reliance on information technology and associated susceptibility to electronic disruption

Version: September 30, 2011 — FOR OFFICIAL USE ONLY — Content: June 2007


U.S. Department of Homeland Security
Protective Security Coordination Division
Office of Infrastructure Protection

Infrastructure Protection Report Series
Resilience One-pager: Business Continuity Plan
March 2012

"Today's hazards require the creation of an ongoing, interactive process that serves to assure the continuation of an organization's essential functions before, during, and after disruptions—whether a major crisis or not." ASIS 2005

UNDERSTAND
ANALYZE
ASSESS
DEVELOP
DEFINE

Business Continuity Planning Process

The development and implementation of a business continuity plan is vital to the overall resilience of any organization. Business continuity is formally defined as a "comprehensive managed effort to prioritize key business processes, identify [hazards] to normal operation, and plan mitigation strategies to ensure effective and efficient organizational response to challenges that surface during and after a crisis" (ASIS 2005). A business continuity plan contributes to reducing organizational consequences and enhancing an organization's ability to continue essential operations after an incident. This document provides an overview regarding the core components of effective business continuity plans and a framework for the development of tailored, organization-specific plans.

Getting Started

The following steps should be completed prior to beginning business continuity planning to best support the long-term success of the plan:

- Ensure senior management supports plan development;
- Define the matters behind developing the plan;
- Develop a policy statement for the eventual use of the plan;
- Commit to incorporating business continuity into the organizational process; and
- Define a planning team to lead the effort (ASIS 2009; BCI 2010).

Once these steps have been taken, the identified team can begin developing the plan.

Developing the Plan

Various business continuity plan methods and resources exist that inform the development of an organization-specific plan (see Additional Resources section). Each organization should follow a methodology that leads to the development of a unique plan that is tailored to its needs. The documentation of these steps, taken together, forms the basis of the plan. Regardless of the approach used, the steps described below should be followed when developing business continuity plans:

- Understand the business;
- Analyze hazards;
- Assess potential consequences;
- Develop mitigation strategies; and
- Define response and recovery capabilities.

Understand the Business

This section of the plan characterizes the essential functions of the organization. The objective is to define what functions are critical to restoring the minimal acceptable operation of the organization. The identified essential functions should be prioritized from most to least critical. Identifying the core operations of the organization requires a thorough understanding of what products and resources the organization relies on to carry out its essential functions. This section should also document the organization's major customers and identify alternate organizations (if any) that could or would supply those customers if it were unable to operate. Lastly, this section should present the objectives and scope of the plan by defining what functions should be protected and considered when implementing response and recovery procedures.

Analyze Hazards

Once the organization's essential functions have been identified, the plan should define the potential hazards (e.g., natural, operational and manmade, or equipment and supply chain failures) that could disrupt operations, always from the perspective of the worst-case scenario. Hazards should be categorized by both their relative frequency and severity. A business continuity plan should address relevant large-scale incidents, such as natural disasters or terrorist attacks, as well as smaller disruptions, such as supply chain partner problems or the absence of key staffers.

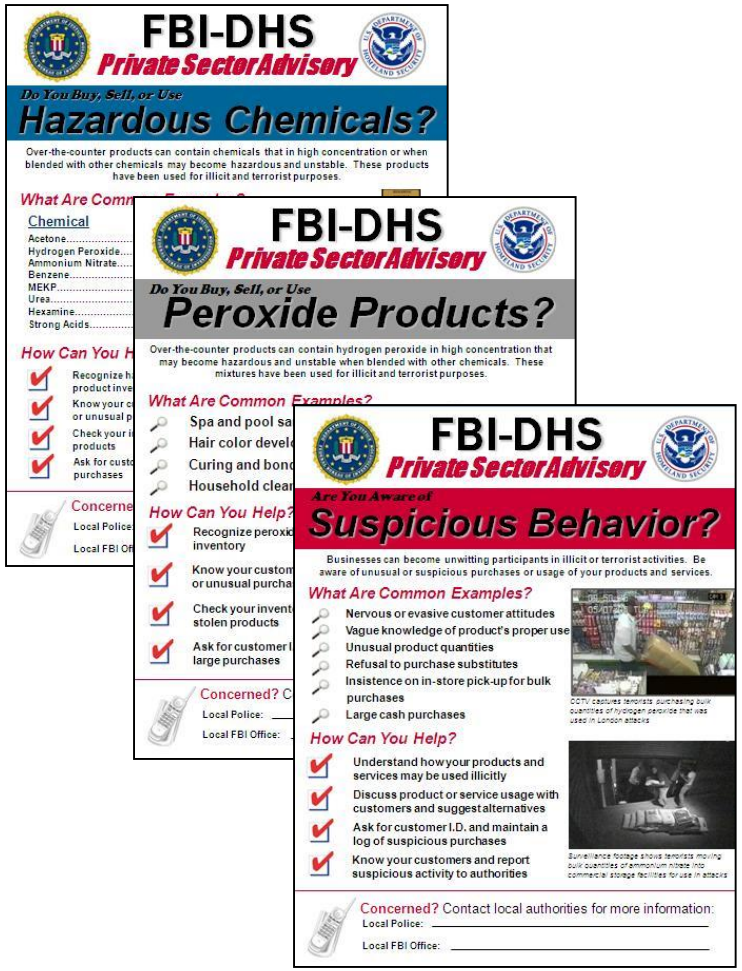
Assess Potential Consequences

Based on the identified hazards, the team should conduct a business impact analysis to evaluate the potential damage or loss to the organization resulting from a disruption (ASIS 2009; BCI 2010; NFPA 2010). To complete this phase, the planning team should (1) define the potential impacts of each of the hazards identified as potentially affecting the critical functions of the organization; and (2) determine the

- The Infrastructure Protection Report Series (IPRS) is developed by the Office of Infrastructure Protection (IP) to increase awareness of the infrastructure mission and build a baseline of security and resilience knowledge throughout the Nation
- The focus of the IPRS is to identify Common Vulnerabilities (CV), Potential Indicators (PI) of Terrorist Activity, and associated Protective Measures (PM), along with actions that can be undertaken to enhance the resilience of critical infrastructure facilities
- Currently under development: IPRS Resilience Series and the IPRS Integrated Reports (CV, PI, PM)

Homeland Security

Bomb-Making Materials Awareness



- Comprehensive effort to educate law enforcement and private sector suppliers of materials used in the manufacture and construction of Improvised Explosive Devices (IED) of the potential risks associated with the sale or theft of those products
  - Point-of-Sale Awareness
  - Notification Processes
  - Supply Chain Awareness
  - Law Enforcement Training Material
- Facilitates partnerships between local law enforcement and private sector
- Encourages the retail industry to take an active role in bombing prevention efforts at little or no cost

Homeland Security

TRIPwire and TRIPwire Community Gateway

- TRIPwire – Online unclassified network for law enforcement having bombing prevention responsibilities to discover and share tactics, techniques, and procedures of terrorist IED use
  - Combines expert analysis with relevant documents gathered from terrorist sources to assist law enforcement's ability to anticipate, identify, and prevent IED incidents
- TRIPwire Community Gateway – Brings timely bombing prevention awareness information and analysis to the private sector with bombing prevention responsibilities
  - Responds to increasing private sector demand for bombing prevention information and assistance
  - Leverages content, expertise, and reputation of the existing TRIPwire system
  - Shares information on common site vulnerabilities, potential threat indicators, and effective protective measures for the 18 critical infrastructure sectors through HSIN-CS

Homeland Security

Risk Mitigation Training

- IED Awareness/Bomb Threat Management Workshop
  - Provides an IED overview and focuses on the steps for managing bomb-related threats by outlining specific mitigation and response strategies to deal with explosive incidents and bomb threats
- IED Search Procedures Workshop
  - Enhances participants' knowledge of IED awareness, prevention measures, and planning protocols by outlining specific search techniques that reduce vulnerability and mitigate the risk of terrorist IED attacks
- Protective Measures Course
  - Provides owners and operators in the public and private sectors with the knowledge to identify the appropriate protective measures for their unique sector
- Surveillance Detection Course for Law Enforcement & Security Professionals
  - Provides participants with the knowledge, skills, and abilities to detect hostile surveillance conducted against critical infrastructure

Risk Mitigation Training (cont.)

- IED Counterterrorism Workshop
  - Enhances the knowledge of State and local law enforcement and public and private sector stakeholders by providing exposure to key elements of the IED threat, surveillance detection methods, and soft target awareness
- Counter-IED/Bomb Threat Management Workshop (Executive Level)
  - High-level workshop, designed for executives and critical infrastructure owners, provides exposure to key elements of the IED threat, soft target awareness, bomb threat management planning**,** and mitigation cost considerations in order to inform risk management planning

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 critical infrastructure protection related concerns
- Enhanced protection and resilience depends on developing and strengthening partnerships between all entities with a role in critical infrastructure protection

Homeland Security

Summary

- Success will depend in part on the strength of our partnership
- Our approach to addressing the terrorism threat will be a long term, ongoing project of the highest priority
- This effort will require the highest degree of vigilance and dedication from all of us

Homeland Security

Homeland Security

For more information visit:
www.dhs.gov/criticalinfrastructure

Frank Westfall

Regional Director

Franklin.Westfall@dhs.gov