The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

Protective Security Advisors and Special Event Domestic Incident Tracker Overview

Federal Emergency Management Agency National Preparedness Symposium

August 8, 2012

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

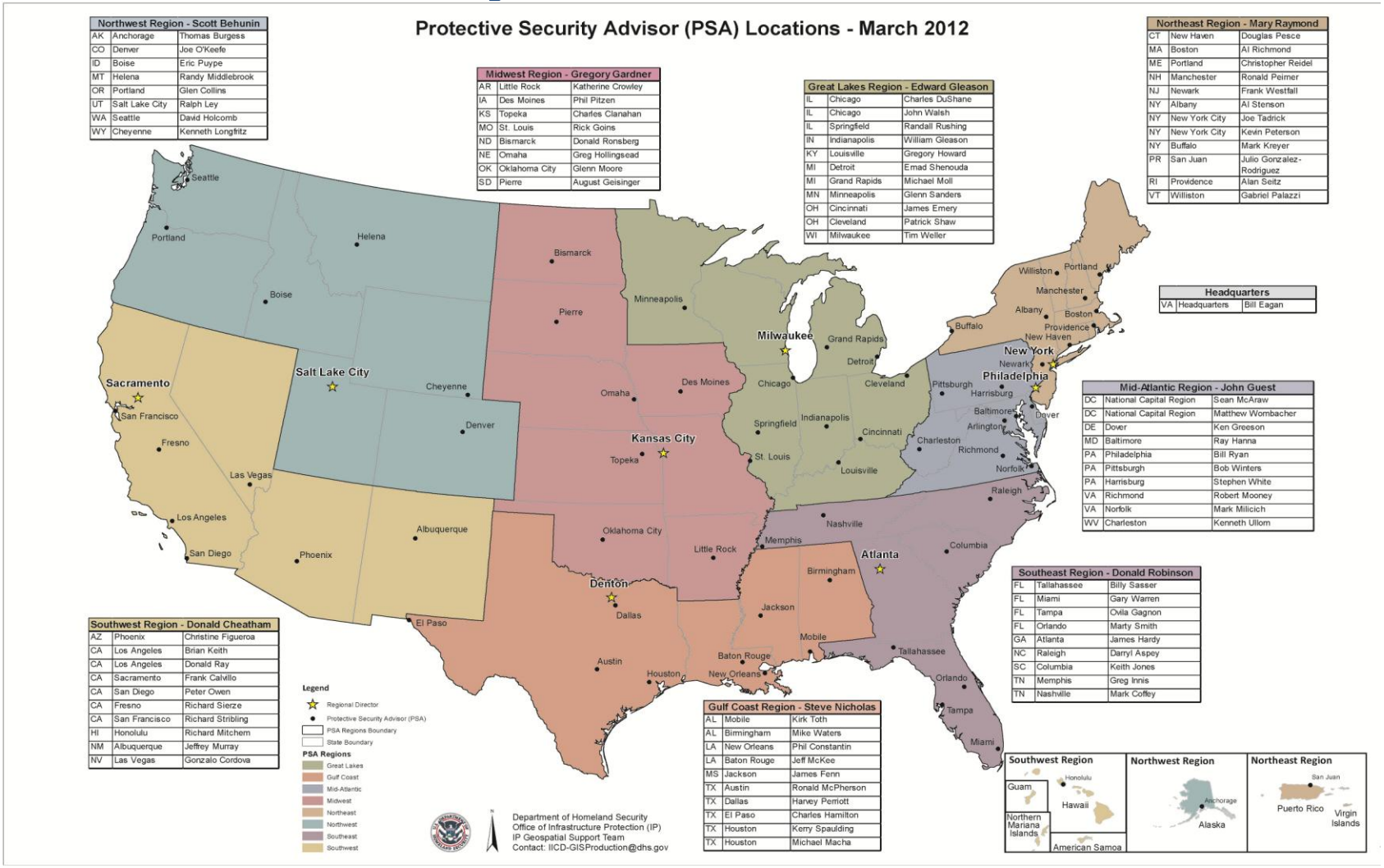
Critical Infrastructure Protection Challenges

- 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 (NPPD/IP) (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

- 93 Protective Security Advisors (PSAs) and Regional Directors, including 87 field deployed personnel, serve as critical infrastructure security specialists
- Deployed to 74 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 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



Homeland Security

ECIP 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
- Enhanced Critical Infrastructure Protection (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 Protected Critical Infrastructure Information program
- Information used by DHS for steady-state analysis and incident management

Homeland Security Information Network

- The 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: Numerous recurring 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

Vulnerability Assessment Programs

- Site Assistance Visits (SAVs)
  - Brings together Federal partners, State and local law enforcement, other emergency responders, and critical infrastructure owners and operators to conduct an “inside the fence” assessment that identifies critical assets, specific vulnerabilities, protective measures, dependencies/interdependencies, and options for consideration for improving security
- Computer Based Assessment Tool
  - A computer-based visual cross-platform tool that displays critical site assets and current security postures
  - Integrates SAV and Buffer Zone Plan assessment data with geospherical video and 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

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 improvised explosive device (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

Risk Mitigation Training

- IED Awareness and 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/private sector 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/private sector stakeholders by providing exposure to key elements of the IED threat, surveillance detection methods, and soft target awareness
- Counter-IED and 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

Special Event and Domestic Incident Tracker

- Introduction
- Objective
- Core Methodology
- Benefits
- Steady State
- Threat Matrix
- Special Event
- Domestic Incident
- Future Vision

SEDIT Introduction

- The Special Event and Domestic Incident Tracker (SEDIT) is a Web-based tool for field-deployed members to enhance steady-state, special event, and domestic incident capabilities
- Applicable to advanced-warning natural hazards, catastrophic planning, and no-notice incidents
- Steady-state data collection allows field members to contribute to special event planning and respond to domestic incidents
- Displays steady-state baseline and mitigated risk for facilities and assets
- Provides predictive analysis regarding dependencies and cascading effects during an event or incident
- Enhances Federal, State, and local situational awareness based on consequence, vulnerability, and threat

SEDIT Introduction (cont.)

- Provides enhanced critical infrastructure information for State and local fusion centers through PSAs
- Tracker uses National Threat Matrix developed with the DHS Office of Intelligence and Analysis (DHS I&A) and has the ability to be modified locally
- Integrates SAV assessments and ECIP survey data in risk calculations
- Incorporates SAV and ECIP resilience data to support domestic incident response

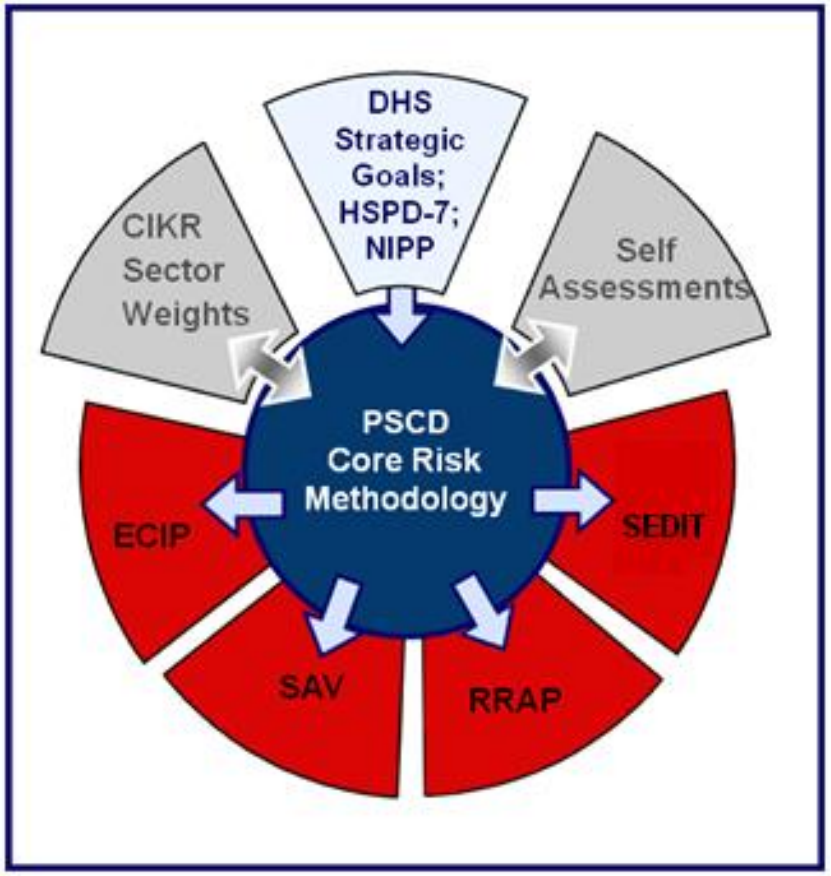
SEDIT Objectives

- Identify and mitigate vulnerabilities at national high priority critical infrastructure facilities
- Support DHS infrastructure protection objectives
  - National Infrastructure Protection Plan – Risk Framework (e.g., develop core assessment methodology): Analyze risk, analyze protective measures in place, mitigation strategies to reduce risk
  - National Response Framework – Infrastructure Liaison: Resilience and dependencies/interdependencies
- Provide meaningful products to owners and operators
  - ECIP Dashboards (e.g., physical security)
  - Relevant Information (e.g., Common Vulnerability, Potential Indicators, and Protective Measure papers)
  - Follow up (e.g., specialized assessment)

Homeland Security

SEDIT Core Methodology

- Aligns methodology to ensure achievement of NPPD/IP and DHS goals
- Capitalizes on existing NPPD/IP processes and tools (e.g., ECIP and SAV)
- Minimizes duplication of effort
- Enhances interaction with the private sector



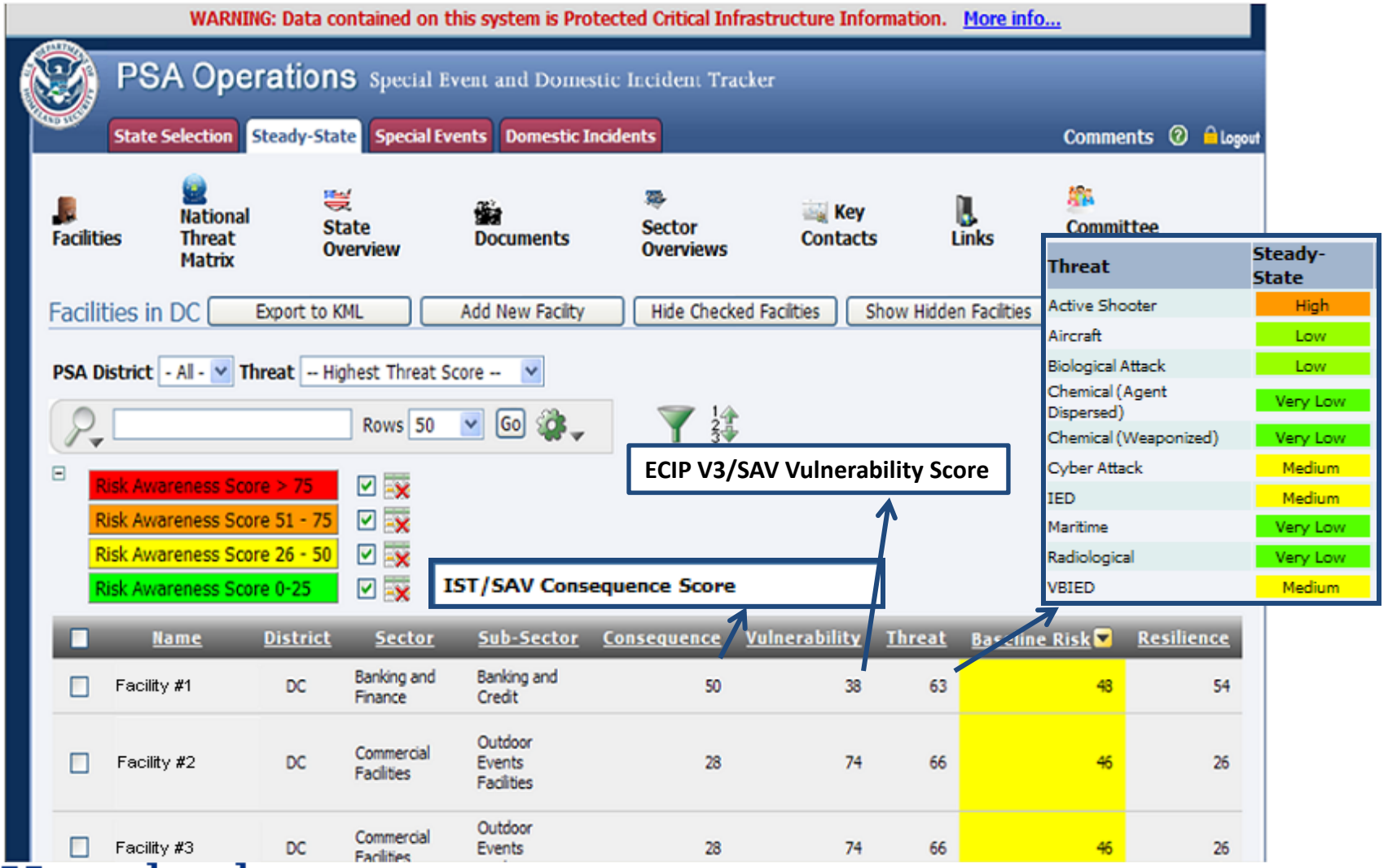
SEDIT Benefits

- Improves information sharing between Federal, State, and local partners and facility owners and operators
- Enhances the Department's ability to analyze data and produce improved protection and resilience measures
  - Risk-based and scalable
  - Allows greater weight to be placed on consequence, vulnerability, or threats
- Presents streamlined and user-friendly functionality in support of special events and domestic incidents
- Increases efficiency in the field by cross-feeding data between steady state (baseline), special events, and domestic incidents

SEDIT Steady State

- Add facilities within each State
- Manipulate the following data within the facility:
  - Facility details
  - Facility Scores (Consequence, Vulnerability, Threat, Baseline Risk and Resilience) based on ECIP/SAV data and the National Threat Matrix
  - Improves risk score based on Consequence Survey function
  - Dependencies
- Information in steady state becomes basis for planning a special event or preparing for a domestic incident through protective and resilience measures

SEDIT Steady State (cont.)

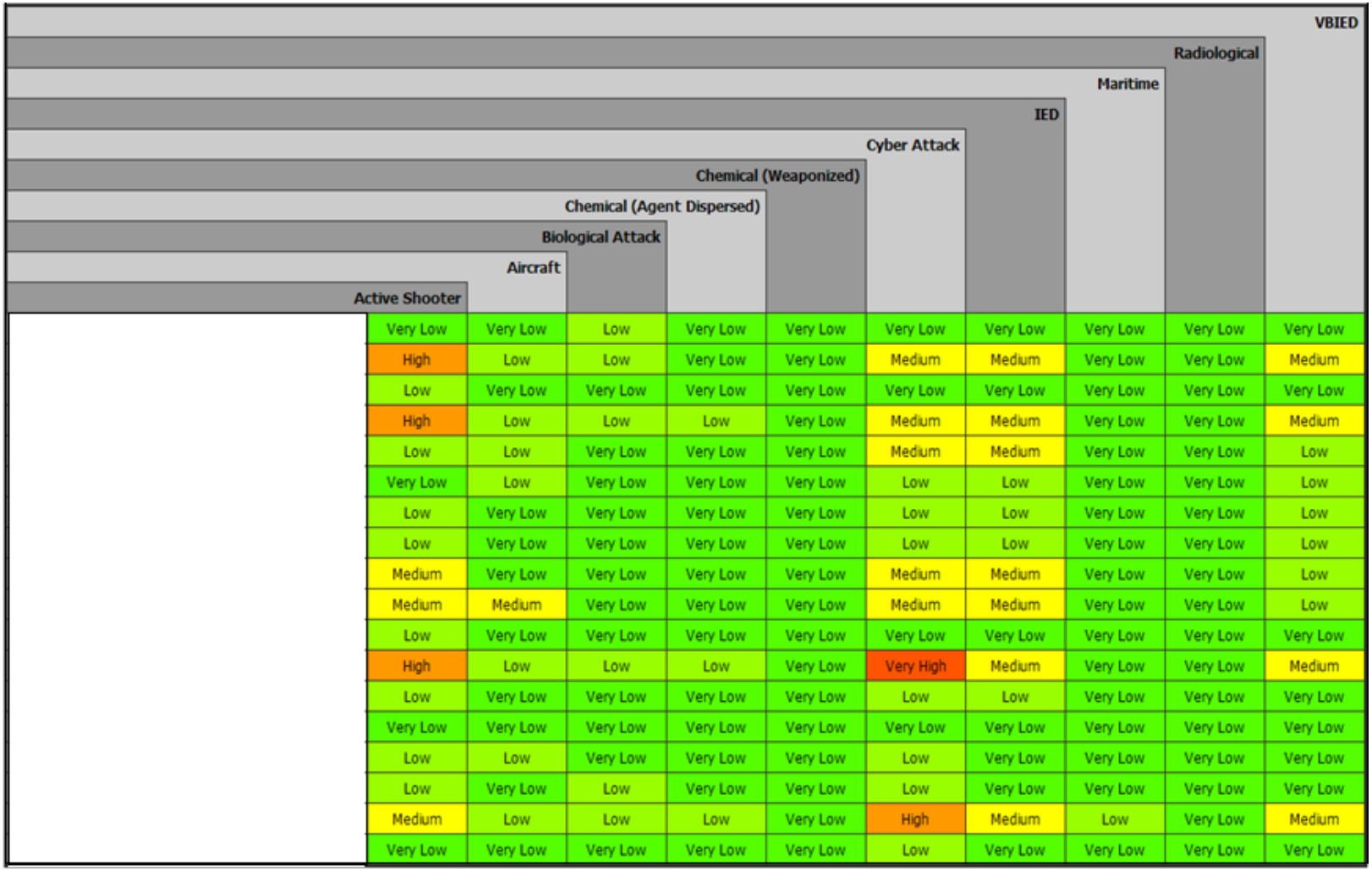


Homeland Security

National Threat Matrix – Steady State

- National Threat Matrix developed by DHS I&A in coordination with Argonne National Laboratory
- Ability to modify facilities in coordination with State and local partners and fusion centers
- National threat information populates facility threat information for special events
- Additional threat streams can be added for special events

National Threat Matrix – Steady State (cont.)



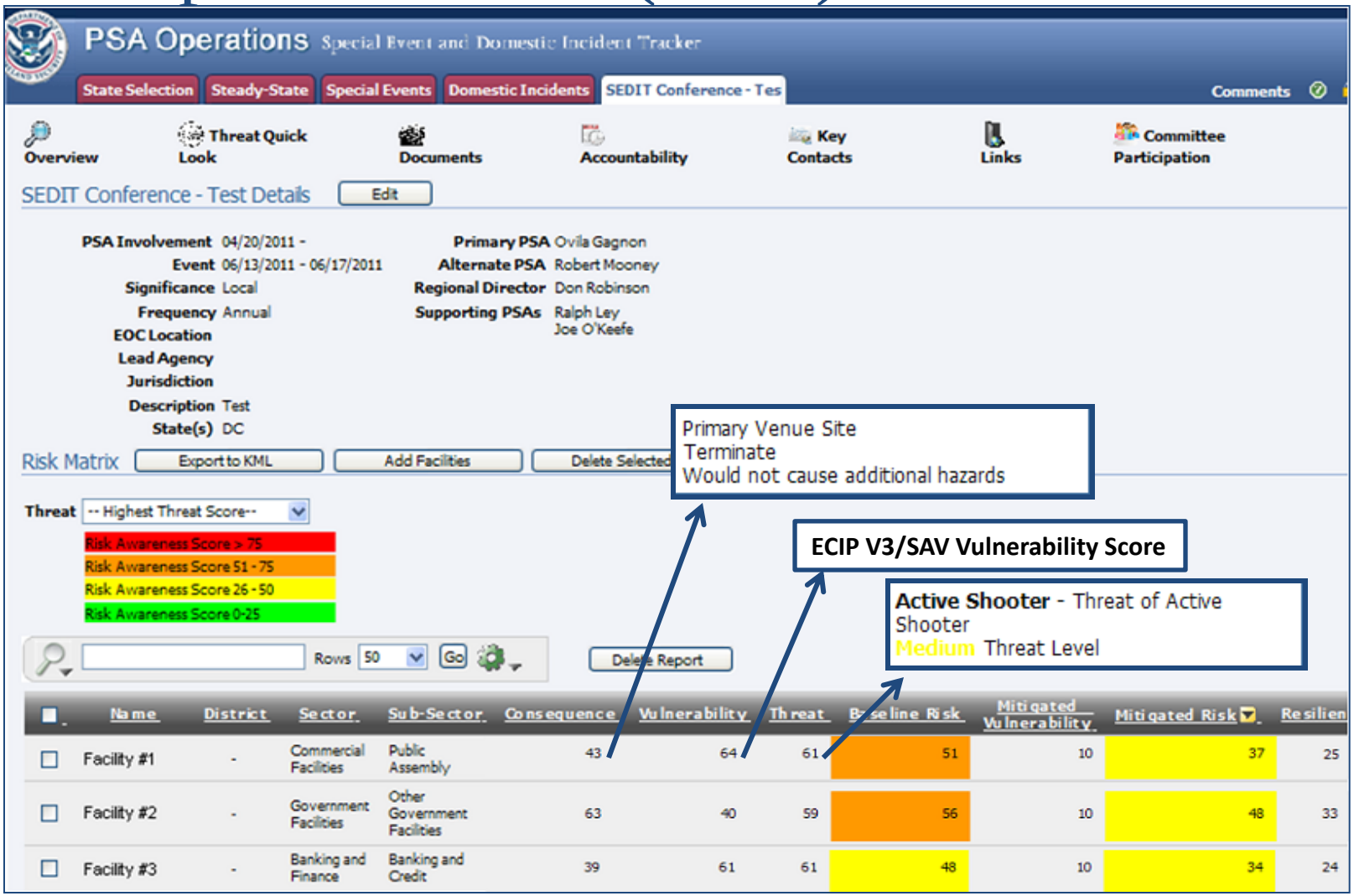
	Active Shooter	Aircraft	Biological Attack	Chemical (Agent Dispersed)	Chemical (Weaponized)	Cyber Attack	IED	Maritime	Radiological	VBIED
	Very Low	Very Low	Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low
	High	Low	Low	Very Low	Very Low	Medium	Medium	Very Low	Very Low	Medium
	Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low
	High	Low	Low	Low	Very Low	Medium	Medium	Very Low	Very Low	Medium
	Low	Low	Very Low	Very Low	Very Low	Medium	Medium	Very Low	Very Low	Low
	Very Low	Low	Very Low	Very Low	Very Low	Low	Low	Very Low	Very Low	Low
	Low	Very Low	Very Low	Very Low	Very Low	Low	Low	Very Low	Very Low	Low
	Low	Very Low	Very Low	Very Low	Very Low	Low	Low	Very Low	Very Low	Low
	Medium	Very Low	Very Low	Very Low	Very Low	Medium	Medium	Very Low	Very Low	Low
	Medium	Medium	Very Low	Very Low	Very Low	Medium	Medium	Very Low	Very Low	Low
	Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low
	High	Low	Low	Low	Very Low	Very High	Medium	Very Low	Very Low	Medium
	Low	Very Low	Very Low	Very Low	Very Low	Low	Low	Very Low	Very Low	Very Low
	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low
	Low	Low	Very Low	Very Low	Very Low	Low	Very Low	Very Low	Very Low	Very Low
	Low	Very Low	Low	Very Low	Very Low	Low	Very Low	Very Low	Very Low	Very Low
	Medium	Low	Low	Low	Very Low	High	Medium	Low	Very Low	Medium
	Very Low	Very Low	Very Low	Very Low	Very Low	Low	Very Low	Very Low	Very Low	Very Low

Homeland Security

SEDIT Special Events

- Key information captured such as description, location, PSA involvement, status, lead agency, significance, and dates
- Add special events in order to take into account real-time threat information and temporary measures as they are put in place
- Catalog primary and secondary venues, lifeline utilities, and supporting infrastructure
- Display baseline risk, mitigated risk, protection measures, and applicable threat scenarios
- Visually display infrastructure in Google Earth format

SEDIT Special Events (cont.)

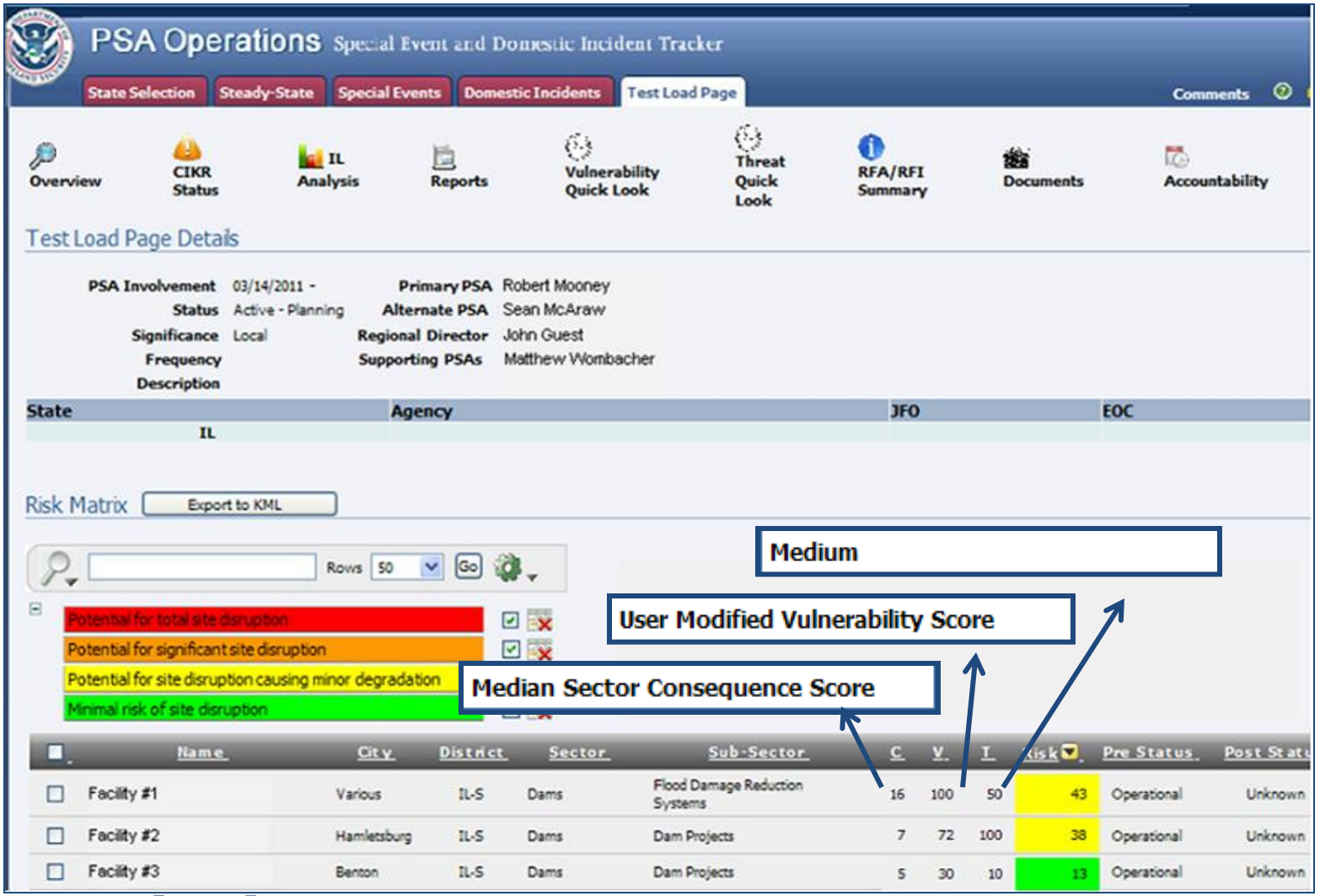


Homeland Security

SEDIT Domestic Incidents

- Key information captured such as description, location, and significance
- Modify vulnerability and threat based on incident impact
- Generate and track Requests for Action (RFAs)/Requests for Information (RFIs)
- Monitor and report on disruption of critical infrastructure
- Provide comprehensive pre- and post-incident information
- Track incidents involving multiple States
- Special events can be exported as a domestic incident
- Visually display infrastructure in Google Earth format
- Track and report infrastructure needs

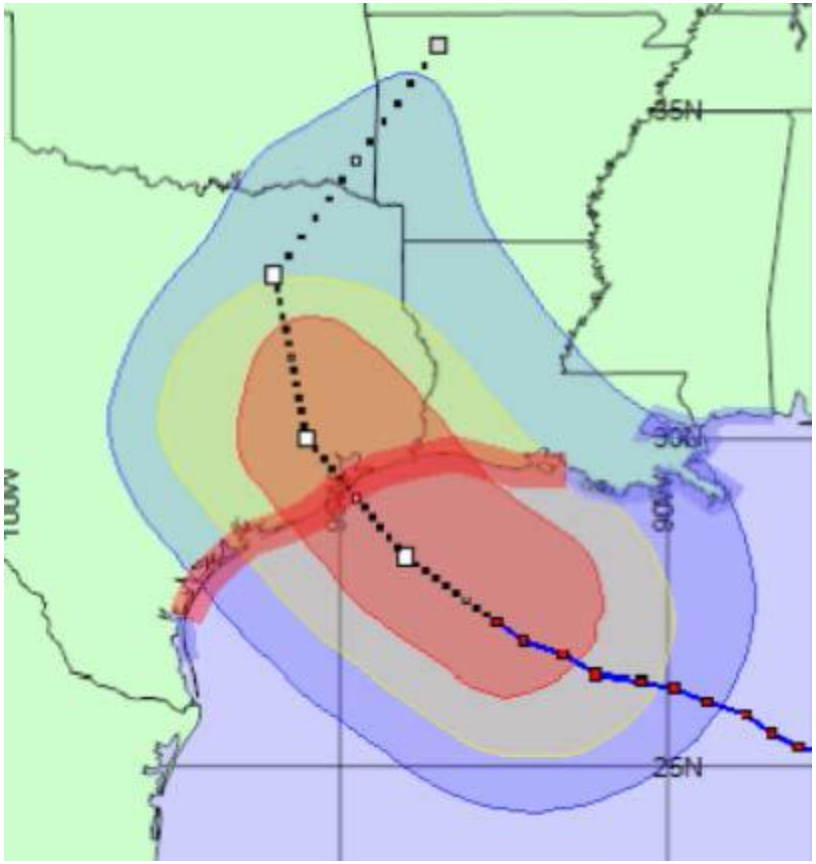
SEDIT Domestic Incidents (cont.)



Homeland Security

Future Updates

- Development of an improved threat matrix. Improvements will include the ability to delete or hide threats from the National Threat Matrix
- Utilize SHAPE files to calculate threat scores for natural disasters based on current or historic modeling
- Link WebEOC to RFI/RFA function in SEDIT



Homeland Security

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

Richard Scott Mitchem

Protective Security Advisor - Honolulu

richard.mitchem@hq.dhs.gov