RISK MANAGEMENT DIVISION:
Critical Infrastructure Protection Efforts

Drug Enforcement Administration

Chemical Industry Conference

Louisville, Kentucky

November 1, 2006

Marybeth Kelliher
Chief, External Affairs Unit
Risk Management Division
Office of Infrastructure Protection
Department of Homeland Security

Challenges to Protecting CI/KR

- 85% of the Nation's critical infrastructure and key resources (CI/KR) are privately owned
  - Robust network of public-private partnerships are crucial to succes of any protection initiative
- Protective programs and risk assessments consume finite resources
  - Prioritization based on risk must be used to guide allocation strategies
- Risk can never be zero, yet resources are limited

RMD Mission and Vision

MISSION

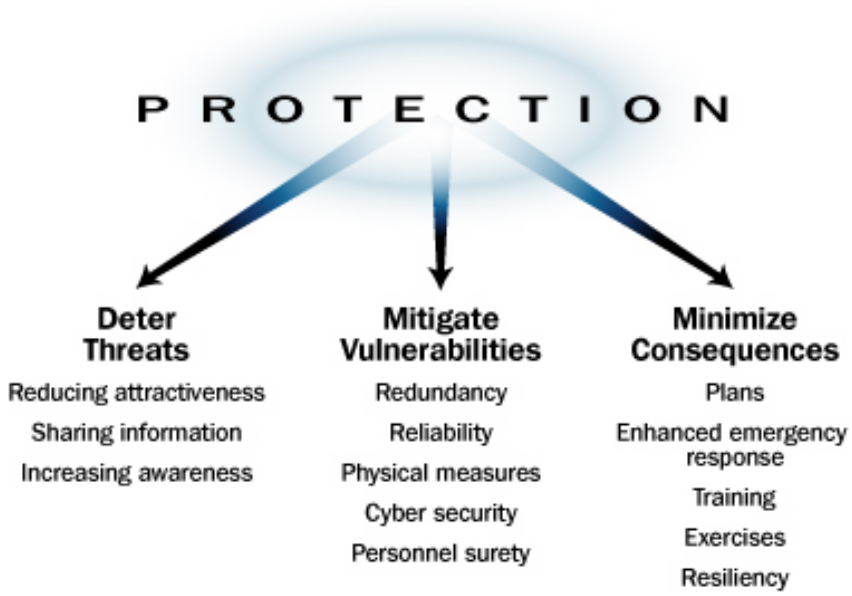
The Risk Management Division will reduce the risk of the Nation's CI/KR to terrorism and deny their use as a weapon by developing, coordinating, integrating, and implementing plans and programs that identify, catalog, prioritize (using a risk-based approach), and protect CI/KR, and that facilitate recovery from all hazards.

VISION

- Inventory the nation's infrastructure and resources through a well-populated National Asset Database (NADB);
- Develop and apply the DHS risk-based prioritization method as part of the National Infrastructure Protection Plan (NIPP) process;
- Oversee and support the execution of the NIPP;
- Maintain a flexible organization that focuses on critical infrastructure protection policy planning and program management;
- Promote a nation-wide protective posture, nurture a flexible response capability, support sector responsibilities, and provide DHS with a near real-time community risk awareness.

NIPP Goal

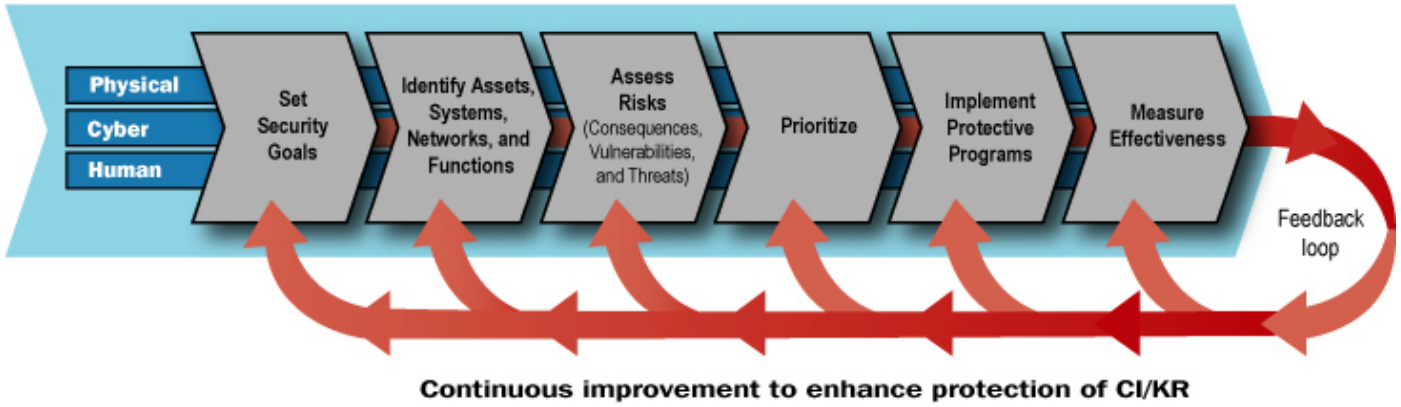
Build a safer, more secure, and more resilient America by enhancing protection of the Nation's CI/KR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and enabling national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.



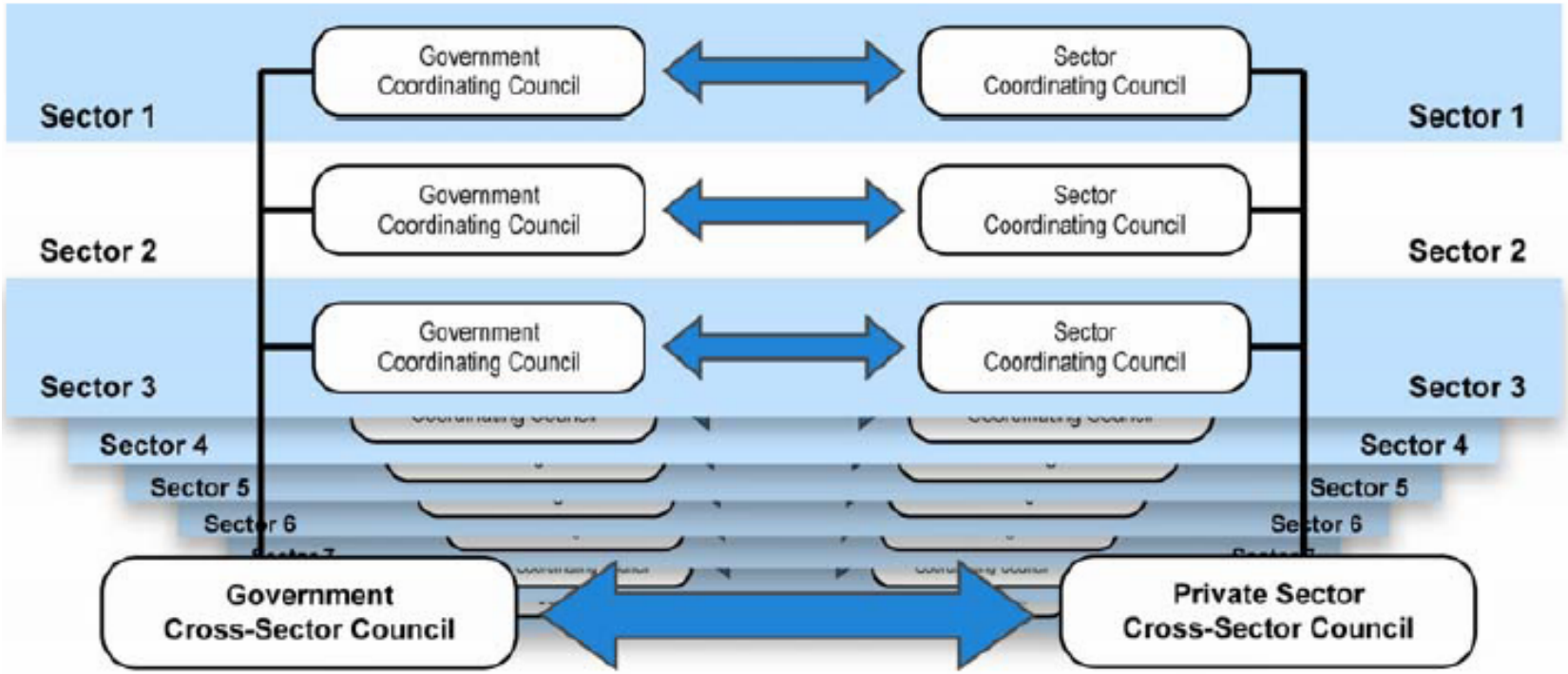
NIPP Risk Management Framework

The NIPP and supporting Sector-Specific Plans (SSPs) describe the processes to:

- Set Security Goals
- Identify Assets, Systems, Networks, and Functions
- Assess Risk (Consequences, Vulnerabilities, and Threats)
- Prioritize
- Implement Protective Programs
- Measure Effectiveness



Sector Partnership Model



Provides the framework for security partners to work together in a robust public-private partnership

DHS/RMD Sector Specific Role

- Directs all risk management activities for the Dams and Commercial Facilities sectors
- Leads protective measure programs for these sectors including:
  - Risk Analysis and Management for Critical Asset Protection activities, Comprehensive Review, Buffer Zone Protection Program, Protective Security Advisors and Site Assistance Visits
- Chairs the Government Coordinating Councils (GCC) for the Commercial Facilities and Dams sectors
  - GCC is composed of representatives from all the federal entities with a stake in CI/KR protection for a specific sector
  - Participates in Sector Coordinating Council (SCC) meetings, the private-sector equivalent of the GCC
- Implements Sector-Specific Plans (SSP) for the Dams and Commercial Facility sectors

Risk Analysis Overview

- Risk = *f* (Consequence, Vulnerability, Threat)
- Risk analysis is part of the overall risk management process:
  - Identify Assets
  - Assess Relative Risk
  - Prioritize for Purpose
- Risk can be analyzed at a variety of levels:
  - Assets
  - Systems
  - Sectors
  - Geographic Areas

Risk Asset & Management For Critical Asset Protection (RAMCAP)

- RAMCAP is the result of a private-public partnership
- Two-part consequence and vulnerability assessment tool for use by a facility owner/operator (O/O)
- Enables the O/O to evaluate both criticality and vulnerability in an accredited fashion and using metrics that will support comparative risk analysis by the U.S. government
- Allows industries to leverage existing risk assessment tools
- Useful stand alone tool for both O/Os and local and state authorities
- Provides O/O with insight into their risk from terrorism, informing their risk management and resource decisions, increasing individual facility security as well as national security

RAMCAP Modules Completed

(Technical Specifications Written)

Commercial Nuclear Power

Petroleum Refineries

Chemical Manufacturing

Nuclear Spent Fuel

LNG Storage

Next RAMCAP Modules

Dams, Locks, and Levees

Water Distribution/Treatment

Comprehensive Reviews

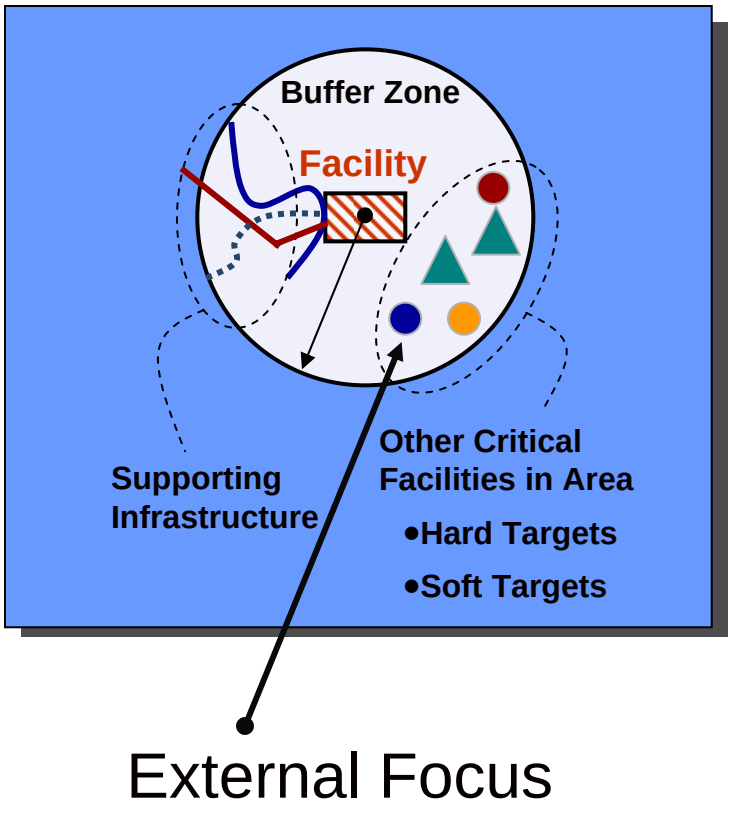
Key Objectives:

- Cooperative government and private sector analysis of high-consequence CI/KR to prevent, mitigate, and respond to catastrophic all-hazard events
- Explore:
  - Exposure to potential terrorist attack
  - Consequences of attack
  - Integrated prevention and response capabilities
- Enhance regional and site security:
  - Short-term protective measures
  - Longer-term risk based security upgrades, investments, decisions

Buffer Zone Protection Program

Key Objectives:

- Make it more difficult for terrorists to conduct surveillance or successfully launch attacks from the immediate vicinity of CI/KR
- To identify and document specific threats and vulnerabilities associated with a facility and surrounding area
- To analyze and categorize the level of risk associated with each vulnerability
- To recommend scalable protective measures that correlate to the Homeland Security Advisory System (HSAS) threat levels
- To illustrate ways in which federal, state and local agencies can most effectively synchronize their preventive actions



Protective Security Advisors

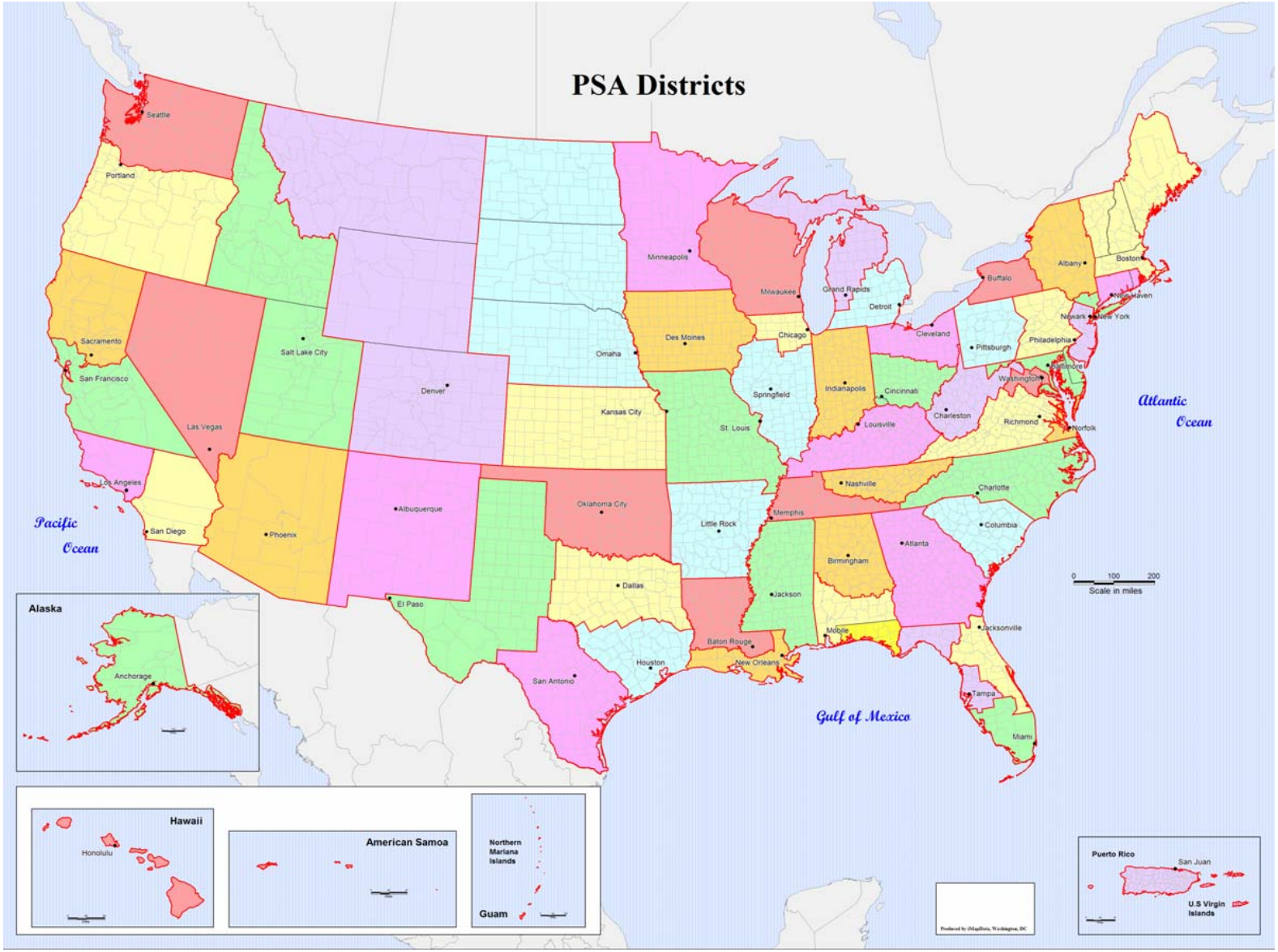
Key Objectives:

- Assist with ongoing local and state critical infrastructure security efforts, as coordinated by the State Homeland Security Advisors
- Support the development of the national risk picture by identifying, assessing, monitoring, and minimizing risk to critical assets at the local level
- Upon request, facilitate and coordinate vulnerability assessments of local CI/KR

Accomplishments to Date:

- 68 PSAs are currently deployed in 60 cities across the U.S.
- 9 Supervisory PSAs have been hired to build up the Program's management structure and oversight of field personnel
- For more information: PSADutyDesk@hq.dhs.gov

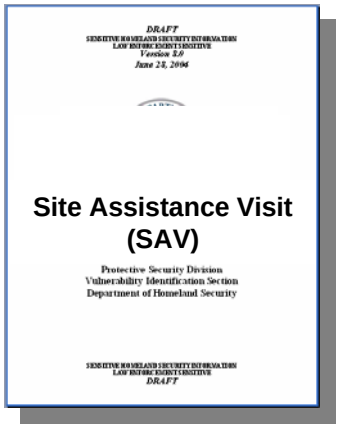
PSA Districts



Site Assistance Visit (SAV)

Key Objectives:

- Identify and document CI/KR vulnerabilities
- Provide information for protective measures planning and resource allocation
- Identify and document protective measures for HSAS threat levels
- Support the threat/vulnerability mapping process
- Provide a foundation for developing common vulnerabilities and potential indicators of terrorism
- Provide private sector with information (comparative statistics, feedback, lessons learned, and best practices)



CV / PI / PM Reports

- A series of reports on specific critical infrastructure sectors to assist owners and operators in detecting and preventing terrorist attacks
  - Characteristics and Common Vulnerabilities (CV) reports provide insights into the common characteristics, the general vulnerabilities, and likely consequences of an attack in a given sector
  - Potential Indicators of Terrorist Activity (PI) reports identify possible signs of an attack to better facilitate early detection, reporting, and prevention of terrorist activities on a sector-by-sector basis
  - Protective Measures (PM) reports describe likely terrorist objectives, methods of attack and corresponding protective measures and their implementation in accordance with the HSAS, on a sector-by-sector basis
- All of these reports are available for use by law enforcement personnel upon request, and as appropriate, to private sector representatives

Bombing Prevention Programs

Key Objectives:

- Consolidate and coordinate national efforts to prevent bombing attacks
- Creation of the Office for Bombing Prevention within RMD
- FY06 initiatives include:
  - Improvised Explosive Device Working Group (IEDWG)
    - Coordinating among the more than 50 IEDWG participants to assess current national programs and initiatives on bombing prevention;
    - Developing a National Strategy for Bombing Prevention; and
    - Overseeing the implementation of recommendation based on the National Strategy
  - TRIPwire: Technical Resource for Incident Prevention
  - Conduct capability analysis for bombing prevention using National Capabilities Analysis Database (NCAD)
  - Multi-Jurisdiction Response Planning (MJRP)

Securing the Chemical Sector

- A $460BN critical infrastructure sector
- Vital to the nation's economy and quality of life, contributing nearly 3% of U.S. Gross Domestic Product (GDP) and generating 6.2MN jobs; a full 5% of America's workforce
- Nation's largest exporting industry with a domestic economic footprint in all 50 states
- Attack, theft, or sabotage at a chemical facility is of concern given the potential for significant health, economic, or national security consequences
- DHS has been directed by Congress to issue interim final chemical security regulations which will be published in the Federal Register by April 2007

Thank You