The Office of Infrastructure Protection

National Protection and Programs Directorate

Department of Homeland Security

Protective Security Coordination Division Overview Brief

August 25, 2011

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 disasters, or other emergencies
- Coordinate the protection of our Nation’s critical infrastructure across all sectors

IP 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

The Threat

We will “hit hard the American economy at its heart and its core.”

- Osama bin Laden

Threats May Come from All Hazards

Critical Infrastructure Defined

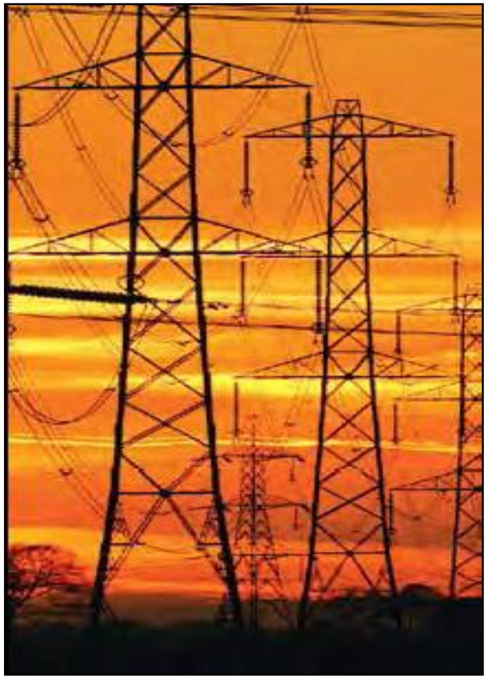
- Critical Infrastructure
  - "Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional,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

Source: National Infrastructure Protection Plan (NIPP) 2009

Homeland Security

Critical Infrastructure Sectors

- Agriculture and Food
- Banking and Finance
- Chemical
- Commercial Facilities
- Commercial Nuclear Reactors, Materials, and Waste
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Drinking Water and Wastewater Treatment Systems
- Emergency Services
- Energy
- Government Facilities
- Information Technology
- National Monuments and Icons
- Postal and Shipping
- Public Health and Healthcare
- Telecommunications
- Transportation Systems



Homeland Security

Critical Infrastructure Protection Challenges

- Majority of critical infrastructure assets are privately-owned
  - DHS has limited legal authority to regulate security practices of private industry (exceptions: high-risk chemical facilities, Transportation Security Administration, United States Coast Guard)
- DHS works with industry and Federal, State, local, tribal, and territorial governments to protect critical infrastructure
  - Coordinated through the NIPP
- To help communities better protect the Nation’s assets, DHS deployed Protective Security Advisors (PSAs) throughout the country

Protective Security Advisors (PSAs)

- 93 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, and territorial link to DHS infrastructure protection resources
  - Coordinate vulnerability assessments, IP products and services, and training
  - Support response, recovery, and reconstitution efforts of States affected by a disaster
  - Provide vital link for information sharing
  - Assist facility owners and operators with obtaining security clearances
- During contingency events, PSAs support the response, recovery, and reconstitution efforts of the State(s) by serving as pre-designated Infrastructure Liaisons (IL) and Deputy ILs at the Joint Field Offices (JFO)
- Developed over 125,000 individual working relationships with Federal, State, local, tribal and territorial critical infrastructure protection partners

Protective Security Coordination Division (PSCD) Risk Mitigation Training

- Provide protection personnel in public and private sectors with specialized security training to prevent and protect against continuing and emerging threats to our Nation’s infrastructure

- Examples of courses include:
  - Surveillance Detection Course
  - Soft Target Awareness Course
  - Protective Measures Course
  - Private Sector Counter-Terrorism Awareness Workshop
  - Improvised Explosive Device Awareness Workshop
  - Bomb-Making Materials Awareness Program

Risk Mitigation Training

- Surveillance Detection Course
  - Provides a guideline for mitigating risks to critical infrastructure through developing, applying, and employing protective measures and the creation of a surveillance detection plan
- Protective Measures
  - Provides the knowledge and skills to understand common vulnerabilities and employ effective protective measures to enhance commercial sector awareness on how to devalue, detect, deter, and defend facilities from terrorism
- Private Sector Counterterrorism Awareness Workshop
  - Provides private sector security professionals with current strategies on soft target awareness, surveillance detection, and IED recognition, and outlines specific counterterrorism awareness and prevention actions that reduce vulnerability and mitigate the risk of domestic terrorist attacks
- Soft Target Awareness Course
  - Provides private sector security and safety personnel terrorism awareness, prevention, and protection information
- IED Awareness Workshop
  - Provides a basic awareness of IED prevention measures and planning protocols and the current technology and trends that characterize IEDs

Protected Critical Infrastructure Information (PCII) Program

- The PCII Program is an important tool to encourage industry to share their sensitive critical infrastructure information
- Established under the Critical Infrastructure Information Act of 2002, the PCII Program protects voluntarily submitted critical infrastructure information from:
  - Freedom of Information Act (FOIA)
  - State and local sunshine laws
  - Civil litigation proceedings
  - Regulatory usage
- Provides private sector with legal protections and “peace of mind”
- To qualify for PCII protections:

  – Information must be voluntarily submitted and not customarily in the public domain

  – Information cannot be submitted in lieu of compliance with any regulatory requirement

Infrastructure Protection Report Series

- Increase awareness and improve understanding of infrastructure protection

Characteristics and Common Vulnerabilities

- Common Characteristics
- Consequences of Events
- Common Vulnerabilities

Potential Indicators of Terrorist Activity

- Surveillance Indicators
- Surveillance Objectives
- Transactional and Behavioral Indicators

Protective Measures

- General Protective Measures Options
- Specific Protective Measures Options per HSAS Level

- DHS has produced reports for <u>142</u> different asset types, including: Casinos, convention centers, hotels, education facilities, office buildings, shopping malls, stadiums, theme parks, residential buildings, and other commercial sector assets

How Can You Help?

- Engage with your PSAs to facilitate protective actions and establish priorities and the need for information
- Assist in efforts to identify, assess, and secure critical infrastructures in your community
- Communicate local critical infrastructure protection related concerns
  - Business and economic ramifications of actions
  - Issues unique to the community

Homeland Security

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

John Guest
Mid-Atlantic Regional Director
John.Guest@hq.dhs.gov