The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

Securing the Nation at the Community Level

CEO Breakfast - Lorain County Safety Council

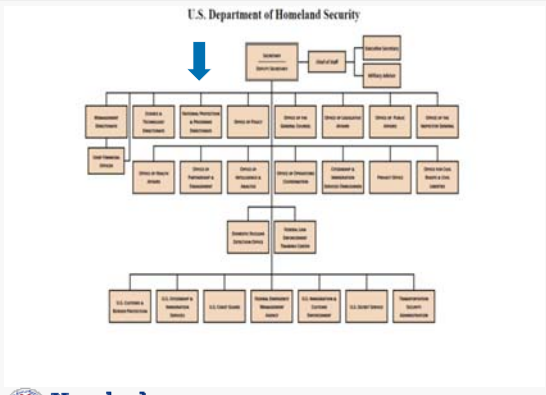
May 9, 2018

Homeland Security

Role of DHS

- 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



Homeland Security

Threats May Come from All Hazards

Courtesy of FEMA

Homeland Security

4

National Preparedness Goal

- Defines what it means for the whole community to be prepared for all types of disasters and emergencies
- The goal is "a more secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk."

Homeland Security

5

National Preparedness Goal (cont.)

5 mission areas

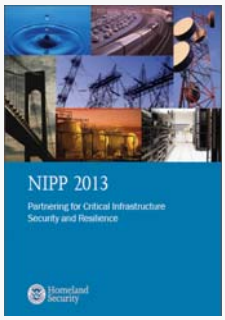
- **Prevention:** Prevent, avoid, or stop an imminent, threatened, or actual act of terrorism
- **Protection:** Protect our citizens, residents, visitors, and assets against the greatest threats and hazards in a manner that allows our interests, aspirations, and way of life to thrive
- **Mitigation:** Reduce the loss of life and property by lessening the impact of future disasters
- **Response:** Respond quickly to save lives, protect property and the environment, and meet basic human needs in the aftermath of a catastrophic incident
- **Recovery:** Recover through a focus on the timely restoration, strengthening, and revitalization of infrastructure, housing, and a sustainable economy, as well as the health, social, cultural, historic, and environmental fabric of communities affected by a catastrophic incident

Homeland Security

6

National Infrastructure Protection Plan (NIPP)

- 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

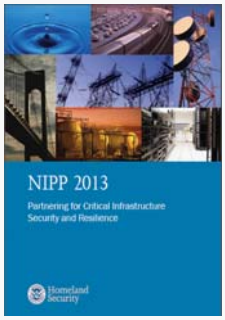


Homeland Security

7

NIPP (cont.)

- Drives internal Department of Homeland Security (DHS) programs and activities
- Guides programs and activities for:
  - Other Federal agencies and departments
  - State, local, tribal, and territorial governments
  - Critical infrastructure owners and operators



Homeland Security

8

Critical Infrastructure Defined

- "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 2013

Courtesy of FEMA

Homeland Security

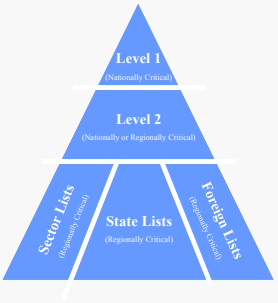
9

Critical Infrastructure Sectors

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

Homeland Security

Infrastructure Prioritization



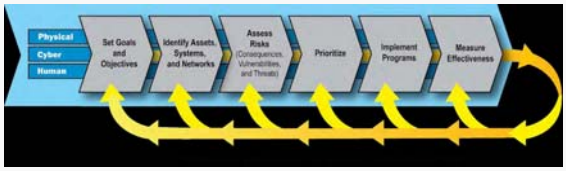
- In accordance with the 9/11 Commission Act, DHS maintains lists of the Nation's most critical infrastructure
- Lists are developed through an annual data call using criteria developed by IP's National Critical Infrastructure Prioritization Program (NCIPP)
- Program identifies domestic and foreign "too critical to fail" infrastructure, which are then used to inform homeland security grant programs, and other critical infrastructure protection activities

Security and Resilience Challenges

- A majority of critical infrastructure is privately owned
- 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, and 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 *(shared responsibility)*

Homeland Security

Risk Management Framework



Continuous improvement to enhance protection of critical infrastructure

Homeland Security

13

Risk: How do we think about risk?

Risk = f(Consequence, Vulnerability, Threat)

CONSEQUENCE (C)	VULNERABILITY (V)	THREAT (T)
Negative effects on public health and safety, the economy, public confidence in institutions, and function of government if asset, system, or network is damaged, destroyed, or disrupted	Likelihood that a characteristic of, or flaw in, an asset, system, or network renders it susceptible to hazards	Likelihood that a particular asset, system, or network will suffer an attack or an incident

RISK

Potential for loss or damage

Homeland Security

14

Protective Security Advisors

- PSAs are field-deployed personnel who serve as critical infrastructure security specialists
- State, local, tribal, and territorial (SLTT) 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

15

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
Access
Handling
Marking
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, or incapacitation of a critical asset
  - Vulnerabilities – Ability to resist threats, including assessments or estimates 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

Protective Security Advisors
Available Services & Resources

Homeland Security

PSA Services: Enhanced Critical Infrastructure Protection Visit (ECIP)

- 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 an Enhanced Critical Infrastructure Protection (ECIP) visit, PSAs focus on coordination, outreach, training, and education
- ECIP visits are often followed by security surveys using the Infrastructure Survey Tool (IST) or Rapid Survey Tool (RST), or delivery of other IP services

Homeland Security

19

PSA Services: Rapid Survey Tool

- The RST is a non-regulatory data collection capability that examines the most critical aspects of a facility's security and resilience posture
- Allows assessors to gather the general status of a facility to determine if an in-depth survey is required
- The data are then analyzed to determine the facility's relative security and resilience in comparison to the national average for similar facilities

Courtesy of DHS

Homeland Security

20

PSA Services: Infrastructure Survey Tool (IST)

- 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

21

Infrastructure Survey Tool (cont.)

- Generates the Protective Measures Index and Resilience Measurement Index
- The tool allows DHS and facility owners and operators to:
  - Identify security gaps
  - Compare a facility's security in relation to similar facilities
  - Track progress toward improving critical infrastructure security

Homeland Security

22

IST 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
  - Intrusion Detection System (IDS)/Close Circuit Television (CCTV)
  - Access Control
  - Security Lighting
- Cyber Vulnerability
- Dependencies*

** Comparative analysis provided*

Homeland Security

23

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

Homeland Security

24

Weighting Process and Participants (cont.)

Fences Example

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

- Wood fence
- 6 feet high
- Partial clear zone
- Fence Protective Measures Index = 13

Courtesy of Public Domain

Homeland Security

25

IST Deliverables

Homeland Security

26

Building Block Approach

ECIP

Facility Dashboard:
- Physical Security
- Security Management
- Security Force
- Information Sharing
- Protective Measures
- Dependencies

IST

Facility Dashboard:
- Physical Security
- Security Management
- Security Force
- Information Sharing
- Protective Measures
- Dependencies
- Threat
- Options for Consideration
- Commendables
- Resiliency Index

RRAP

Multiple Dashboards:
- Physical Security
- Security Management
- Security Force
- Information Sharing
- Protective Measures
- Dependencies
- Threat
- Options for Consideration
- Commendables
- Resiliency Index
- Interdependencies
- Regional PMI
- Regional RI

27

PSA Services: 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

Homeland Security

28

PSA Coordination: National Infrastructure Coordinating Center (NICC)

- http://www.dhs.gov/national-infrastructure-coordinating-center
- The National Infrastructure Coordinating Center (NICC) is the information and coordination hub of a national network dedicated to protecting critical infrastructure
- 24/7 situational awareness and crisis monitoring of critical infrastructure
- Shares threat information in order to reduce risk, prevent damage, and enable rapid recovery of critical infrastructure assets
- The NICC and the NCCIC are co-located to facilitate collaboration

Homeland Security

29

DHS Cyber Security Available Services & Resources

Homeland Security

30

DHS Cyber Security

- DHS is responsible for safeguarding our Nation's critical infrastructure from physical and cyber threats that can affect national security, public safety, and economic prosperity.
- DHS actively engages the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm these strategic assets.

Homeland Security

31

DHS Cyber Security Resources: Cyber Infrastructure Survey Tool

- The Cyber Infrastructure Survey Tool (C-IST) provides public and private sector organizations with:
  - Effective, repeatable data collection technique for cybersecurity operations
  - Ability to review results using comparative data analytics and peer metrics
  - User-friendly, data-rich, interactive dashboard for sharing information on and planning improvements to Critical Cyber Services (CCS)
  - Note: C-IST's are conducted by CSA's

Homeland Security

32

Cyber Security Evaluation Tool (CSET®)

- Stand-alone software application
- Self-assessment using recognized standards
- Tool for integrating cybersecurity into existing corporate risk management strategy

CSET Download:

http:/us-cert.gov/control_systems/csetdownload.html

Homeland Security

33

National Cybersecurity Assessments and Technical Services Team (NCATS)

- The NCATS team consists of subject matter experts in penetration testing methodology and tactical delivery
- Washington, D.C. based *(National Cybersecurity and Communications Integration Center – NCCIC)*
- NCATS team members have extensive experience in current and emerging web applications, networks, databases, wireless, mobile computing, cloud security, social engineering, social media and intelligence gathering

Homeland Security

34

NCATS Services

NCATS security services currently available include:

- Vulnerability Scanning and Testing
- Penetration Testing
- Social Engineering (Phishing)
- Web Application Scanning and Testing
- Operating System Scanning
- Database Scanning
- Wireless Discovery and Identification

Homeland Security

35

Cyber Incident Reporting

- NCCIC provides real-time threat analysis and incident reporting capabilities
  - **24x7 contact number: 1-888-282-0870**
  - Email: nccic@hq.dhs.gov
- When to report:
  - If there is a suspected or confirmed cyber attack or incident that:
    - Affects core government or critical infrastructure functions
    - Results in the loss of data, system availability, or control of systems
    - Indicates malicious software is present on critical systems

Homeland Security

36