The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

Protective Security Coordination Division Overview

32nd Annual Dakota Conference on Rural and Public Health

14 June 2017

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

2

Threats May Come from All Hazards

Courtesy of FEMA

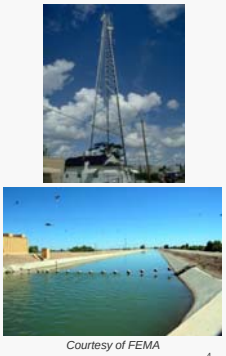
Homeland Security

3

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

4

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

Courtesy of DHS

Homeland Security

5

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

Homeland Security

6

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

Protective Security Coordination Division

- Based within the National Protection and Programs Directorate's (NPPD) Office of Infrastructure Protection (IP), the Protective Security Coordination Division's (PSCD) mission is to:
  - Proactively engage with Federal, State, local, tribal, and territorial (FSLTT) government mission partners and members of the private sector stakeholder community to protect the Nation's critical infrastructure

Homeland Security

PSCD Mission Areas

- Conduct Security Surveys, Gap Analysis, and Assessments
- Conduct Outreach Activities
- Support National Special Security Events (NSSEs) and Special Event Activity Rating (SEAR) Events
- Respond to Incidents
- Provide Improvised Explosive Device (IED) Awareness & Risk Mitigation Training

Homeland Security

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

Protective Security Advisor Locations

Courtesy of DHS

Homeland Security

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."

Courtesy of DHS

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

Infrastructure Survey Tool

- 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

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

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*

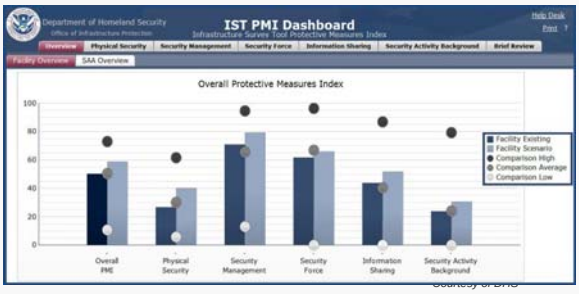
Homeland Security

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

IST Deliverables



Courtesy of DHS

Homeland Security

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

19

IP Gateway

- https://ipgateway.dhs.gov/
- The IP Gateway is a single interface through which DHS mission partners can access a large range of integrated IP systems and capabilities to conduct comprehensive data collection and analysis
- It enables SLTT and Federal partners to manage information about the infrastructure in their communities for risk management, infrastructure protection, event planning, and incident response activities

Homeland Security

20

InfraGard

- https://www.infragard.org
- InfraGard is an information-sharing and analysis effort serving the interests of 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 (FBI) 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

21

Homeland Security Information Network (HSIN)

- https://hsin.dhs.gov/
- HSIN is DHS's primary technology tool for trusted information sharing
- HSIN – Critical Infrastructure (HSIN-CI) enables direct communication between:
  - DHS
  - Federal, State, and local governments
  - Critical infrastructure owners and operators

Homeland Security

22

Homeland Security Information Network (cont.)

- Content includes:
  - Planning and Preparedness: Risk assessments, analysis, guidance, and security products; geospatial products and hurricane models; and 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

23

Cyber Support for Critical Infrastructure

- National Cybersecurity and Communications Integration Center (NCCIC)
  - United States Computer Emergency Readiness Team (US-CERT) Operations Center
  - Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Operations Center
  - National Cybersecurity Assessment & Technical Services (NCATS)
- US-CERT
- Control Systems Security Program
- Cyber Exercise Program
- Cyber Security Evaluations Program
- Cyber Security Advisors
- Protective Security Advisors

Homeland Security

24

Critical Infrastructure Cyber Community

- www.us-cert.gov/ccubedvp
- DHS launched the C³ Program in February 2014 to complement the launch of the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
- The C³ Voluntary Program helps sectors and organizations that want to use the CSF by connecting them to existing cyber risk management capabilities provided by DHS, other U.S. Government organizations, and the private sector
- The C³ website describes the various programs DHS offers to critical infrastructure partners, including Federal, SLTT, and private sector organizations

Homeland Security

Cyber Incident Reporting

- NCCIC provides real-time threat analysis and incident reporting capabilities
  - 24x7 contact number: 1-888-282-0870
  - https://forms.us-cert.gov/report/
- 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

Cyber Incident Reporting (cont.)

Courtesy of CS&C

- Malware Submission Process:
  - Please send all submissions to the Advance Malware Analysis Center at submit@malware.us-cert.gov
  - Must be provided in a password-protected zip files using password "infected"
  - Web-submission: https://malware.us-cert.gov

Homeland Security

Other Products and Services

First Responder Support Tools (FiRST) Application

Courtesy of DHS OBP

- Geospatial smartphone application developed by OBP and DHS Office of Science and Technology
- Vetted access for Federal and State government users
- Quickly determine IED safe stand-off distances, potential damage, roadblock locations, mandatory evacuation or shelter zones, and nearby facilities of concern

Homeland Security

Summary

- Provide partners with effective vulnerability and gap analyses, bombing prevention capability analyses, and the development of protective measures to identify emerging needs and areas for investment
- Through data collection, assessment, and analysis, DHS can generate products for Federal, State, and local officials and private sector owners and operators that drive initiatives, such as infrastructure protection grant programs and research and development requirements

Homeland Security

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

Homeland Security


Homeland Security
For more information, visit:
www.dhs.gov/critical-infrastructure
Don Ronsberg
Protective Security Advisor, ND District
Donald.ronsberg@hq.dhs.gov
Homeland Security