SECURING CRITICAL INFRASTRUCTURE FROM INSIDER THREATS

NITSIG 2019 INSIDER THREAT SYMPOSIUM & EXPO

CISA
CYBER+INFRASTRUCTURE

Welcome & Introductions

Daniel Abreu

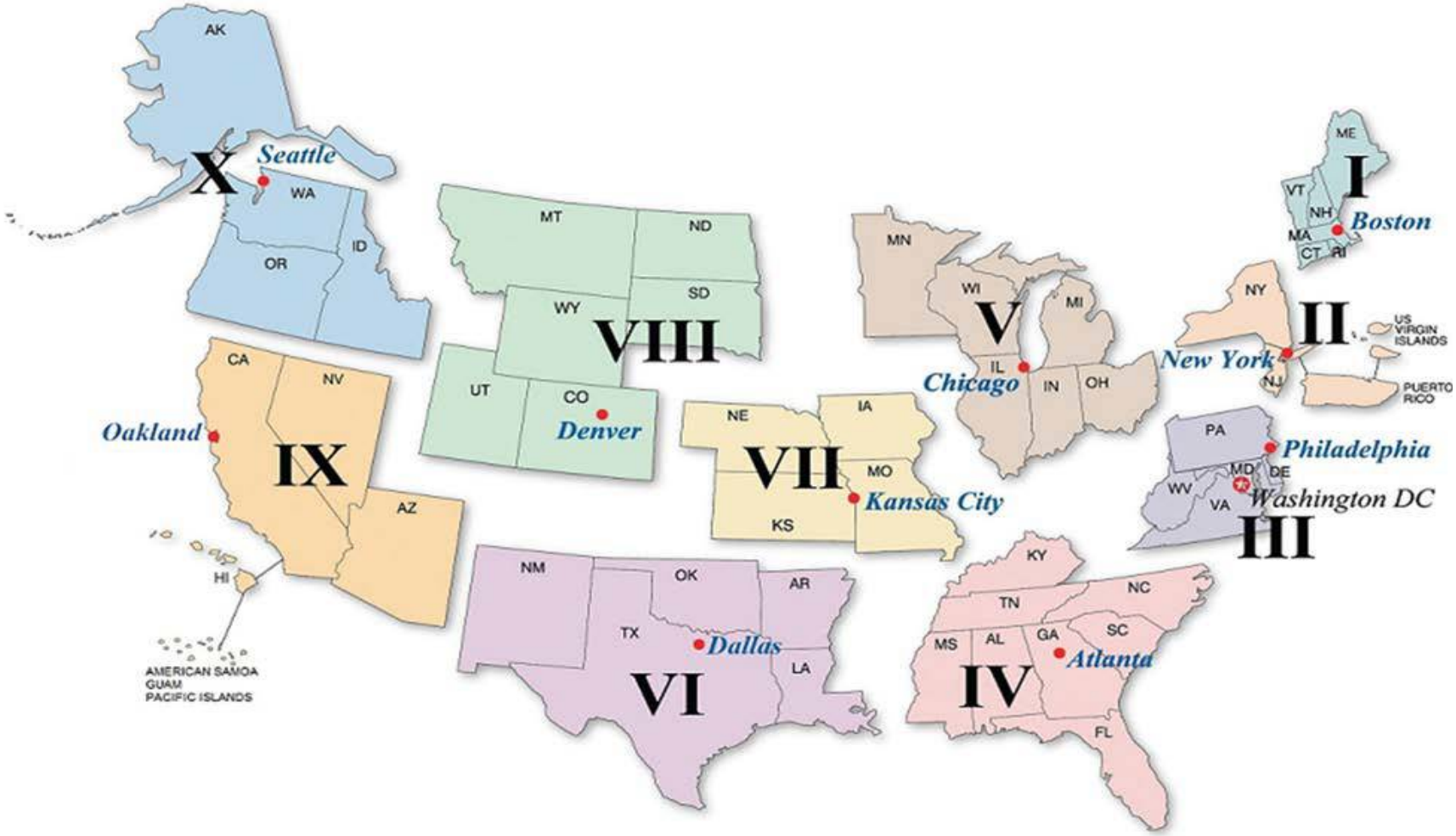
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

We are the Nation's Risk Advisors

The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure

Regions and Regional Office Locations



Director's Priorities

1) China, Supply Chain, and 5G

China presents the most pressing long-term strategic risk to the United States. CISA is looking to reduce the risks of Chinese supply chain compromise, whether that is through 5G or any other technologies.

2) Election Security

CISA is responsible for assisting state and local governments, and the private sector organizations that support them, with their efforts to enhance the security and resilience of election infrastructure. CISA's objective is to reduce the likelihood of compromises to election infrastructure confidentiality, integrity, and availability.

Director's Priorities

3) Soft Target Security

Intentional targeting of soft targets and crowded places undermines traditional risk management and physical security practices by deliberately exploiting vulnerabilities. As the DHS lead for the soft targets and crowded places security effort, CISA supports partners to identify, develop, and implement innovative and scalable measures to mitigate risks to these venues.

4) Federal Cybersecurity

CISA leads the Federal Government in confronting this challenge with a unity of purpose that drives federal agencies to make risk informed cybersecurity decisions. CISA's authorities present the capability and opportunity to create federal cybersecurity approaches that address the speed of change.

Director’s Priorities

5) Industrial Control Systems

Much of critical infrastructure shares a common characteristic: a dependence on industrial control systems (ICS). ICS control, monitor, and manage essential functions for a wide array of critical infrastructure. CISA leads the Federal Government’s unified effort to work with the ICS community to reduce risk to our critical infrastructure by strengthening control systems’ security and resilience.

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Infrastructure Security Division

Infrastructure Security Division leads the coordinated effort to reduce risks posed to our critical infrastructure, whether from man-made or natural causes.

MISSION PRIORITIES:

- Securing critical infrastructure from terrorist attacks.
- Working with government and private sector partners to increase security around soft targets and crowded places through training, exercises, assessments and other resources
- Collaborating with government partners to share security best practices, conduct assessments and share information related to school safety
- Preventing complex or hybrid attacks in a converging cyber-physical threat landscape
- Managing regulatory compliance of securing chemical facilities through the Chemical Facility Anti-Terrorism Standards program.

Capabilities and Programs

Capability Summary

- Vulnerability assessment
- Advisory services
- Information sharing
- Guidance/standards development
- Regulatory administration
- Inspections
- Technical assistance
- IT tools and services
- Training
- Exercises
- Coordination and management
- Capability/requirements assessment
- Security planning

Program Summary

- Soft Targets and Crowded Places
- School Safety
- Bombing Prevention
- Protective Security Advisors
- Chemical Facility Anti-Terrorism Standards (CFATS) and Chemical Security
- TRIP*wire*
- Interagency Security Committee
- Vulnerability Assessments and Regional Risk Assessments
- IP Gateway and Homeland Security Information Network-Critical Infrastructure
- Sector Expertise
- National Infrastructure Protection Plan (NIPP) Management
- Security Training & Exercises
- Incident Response & Recovery Programs

CISA
CYBER+INFRASTRUCTURE

Insider Threat Mitigation Program

Why:

•All organizations are vulnerable to the threat that insiders may use their access to compromise information, disrupt operations, or cause physical harm to employees.

•To mitigate this threat, organizations are encouraged to establish and maintain a comprehensive insider threat program that protects physical and cyber assets from intentional or unintentional harm.

Viewpoints:

•Private Sector: Options for Consideration

•Federal Government: Standards

•Regulatory: Chemical Personnel Surety

Perspectives:

•Cyber

•Workplace Violence

•Ideology

Mitigating the Insider Threat

Steps that organizations can take to establish an insider threat program that assists in identifying and protecting critical assets, recognizing and reporting suspicious behavior, and assessing and responding to insider threats:

Establish a Program

- Designate a Senior Manager
- Form an Insider Threat Working Group
- Develop Governance and Police Document
- Implement a Formal Training and Awareness Program
- Create an Insider Threat Program Office

Protect Assets

- Identify and Document Organizational Assets
- Prioritize Critical Assets Requiring the Most Protection

Recognize and Report

- Develop an Understanding of Behavior Norms and standard Business Activity
- Be Aware of High-Risk Behavior That Can Indicate a Potential Insider Threat
- Establish Clear Guidelines for Reporting Suspicious Behavior

Identifying the Threat

No standard profile – impacted by:

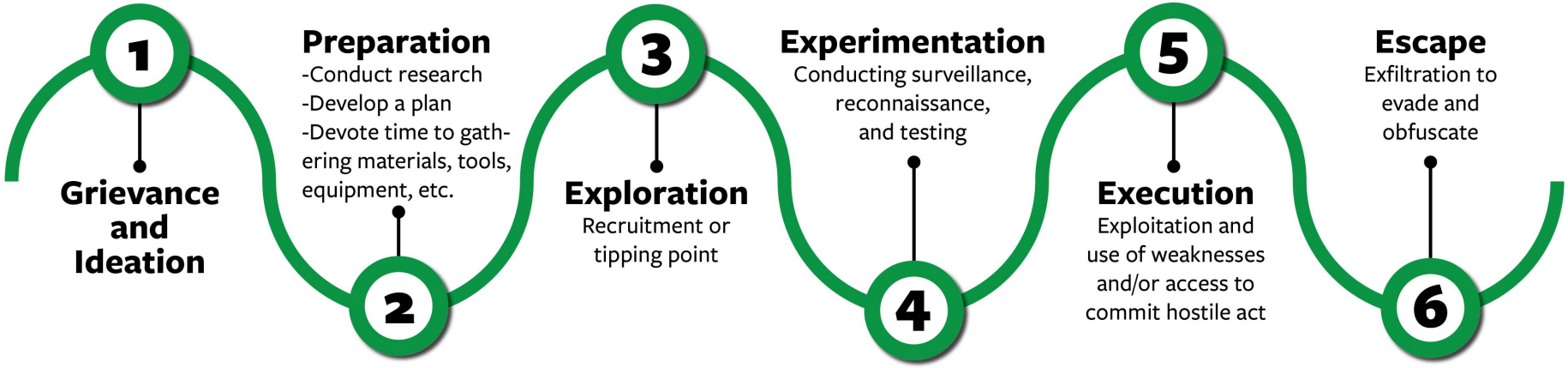
Personal Predispositions • Contextual Stressors • Patterns of Suspicious Behaviors and Actions

Seldom act impulsively

Moving from Idea to Action

Red flags involve changes in baseline behavior

Usually exhibit observable patterns



Assess and Respond

- Implement a System to Collect and Correlate Data
- Develop Detection Indicators Based on Data Source
- Form a Threat Management Team to Analyze Suspicious Behavior
- Establish Procedures For Recommending an Appropriate Response

Threat Management Team

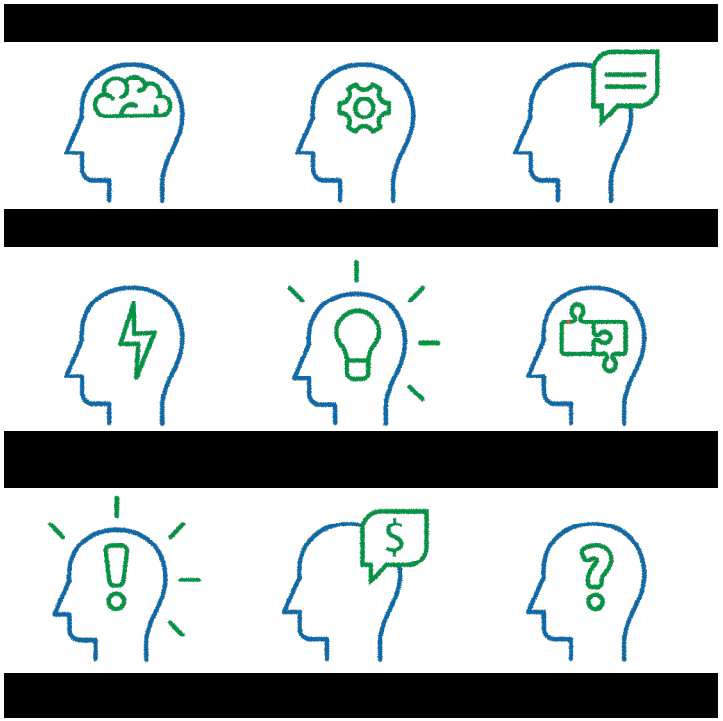
- Your team should align to company culture, structure, business, and characteristics
- Ensure multi-disciplinary approach
  - **Leverage organic and existing functions**
  - **Involve external resources on case-by-case basis**
  - **Gather information from trusted sources**
  - **For some entities of sufficient size, complexity, or risk, consider dedicated resources**
- The "truth is out there" and can be ascertained through inclusion and totality assessment

Threat Mitigators

Gather and assess **information** that may lower or mitigate risk

Threat mitigators are protective factors present in a subject and consist of:

- **Persons, things, and/or circumstances** that may reduce likelihood of hostile act
- **Personal traits** that enhance ability to cope with stressors
- **External factors that reduce risk** (in relation to subject, target, environment)
- **Expressions of remorse**
- **Positive response to limits** imposed or actions taken
- **Self-imposed problem solving** or professional treatment
- **Assess the services offered** and which have been accessed/used



Manage

- Goal is to help the person of concern and prevent a hostile insider act
- Prevention is holistic – subject, target, and organizational setting/situation
- Case management includes active and passive intervention strategies
- Multiple management strategies are often appropriate, representing different disciplines of the Threat Management Team
- Effective management must be sustained

Intervention

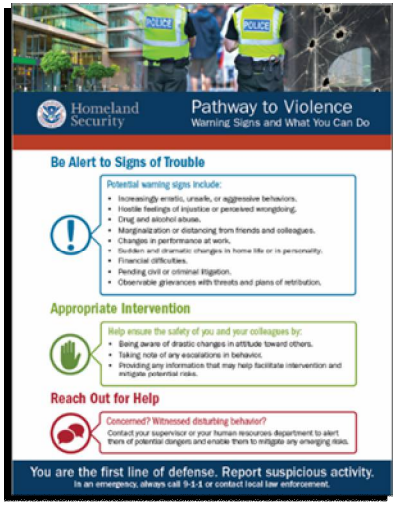
Consider a range of passive and active strategies geared toward preventing insider threat actions

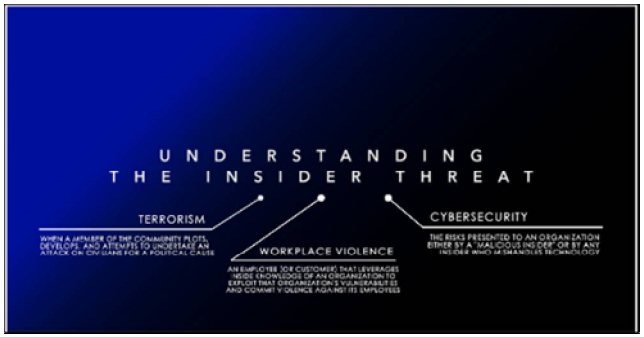
- Take no action
- Watch and wait
- Employee Assistance Program (EAP) referral
- Drug and alcohol testing
- Performance assessment
- Medical attention or counseling
- Third party monitoring
- Interview with supervisor and coworkers
- Direct interview

- Monitoring and investigation – employee records, social media, computer/network activity
- Physical/information security measures
- Violence risk assessment
- Target risk reduction
- Administrative actions – disciplinary, leave, reassignment, safe termination
- Law enforcement involvement
- Legal actions (civil or criminal)

Resources

- Resources:
  - Insider Threat Mitigation Website
  - Insider Threat Mitigation Fact Sheet
  - Insider Threat Mitigation Video
  - Pathway to Violence Video
  - Pathway to Violence Fact Sheet
  - IS-915 Insider Threat Training
  - Active Shooter Preparedness
- Upcoming:
  - Insider threat guide
  - Fact sheet for human resources
  - Field delivered threat management team training





https://www.dhs.gov/insider-threat-mitigation

Contact

For More Information:
https://www.dhs.gov/insider-threat-mitigation

Contact:
InTmitigation@hq.dhs.gov