CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

YOUR LOCAL …
HOMELAND SECURITY RESOURCES

Baltimore City LEPC Meeting

December 7, 2021

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

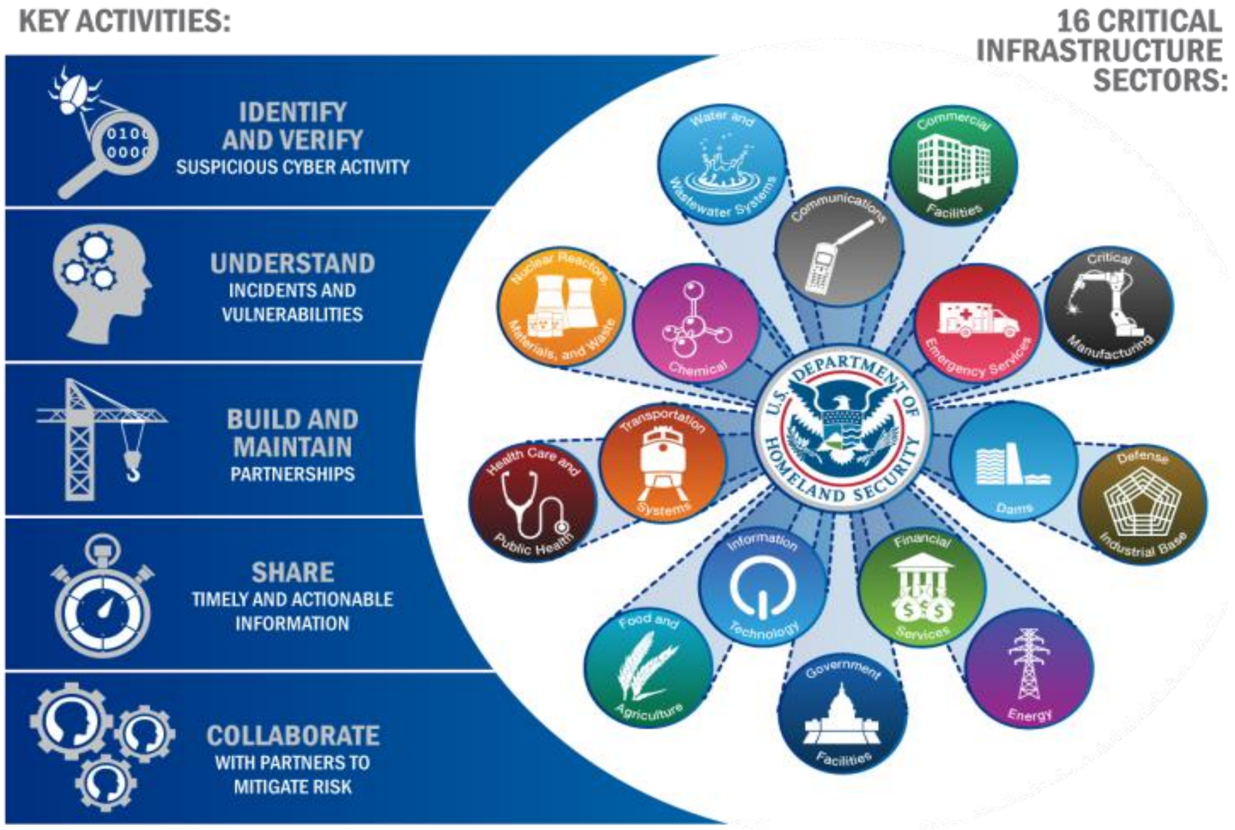
Secure and resilient critical infrastructure for the American people.

MISSION

Lead the national effort to understand and manage cyber and physical risk to our critical infrastructure.

Critical Infrastructure Significance

- ✓ Critical Infrastructure refers to the assets, systems, and networks, whether physical or cyber.
- ✓ So vital to the Nation, that their incapacitation or destruction would have a debilitating effect on:
  - National Security
  - The Economy
  - Public Health or Safety
  - Our Way of Life



KEY ACTIVITIES:

IDENTIFY AND VERIFY SUSPICIOUS CYBER ACTIVITY

UNDERSTAND INCIDENTS AND VULNERABILITIES

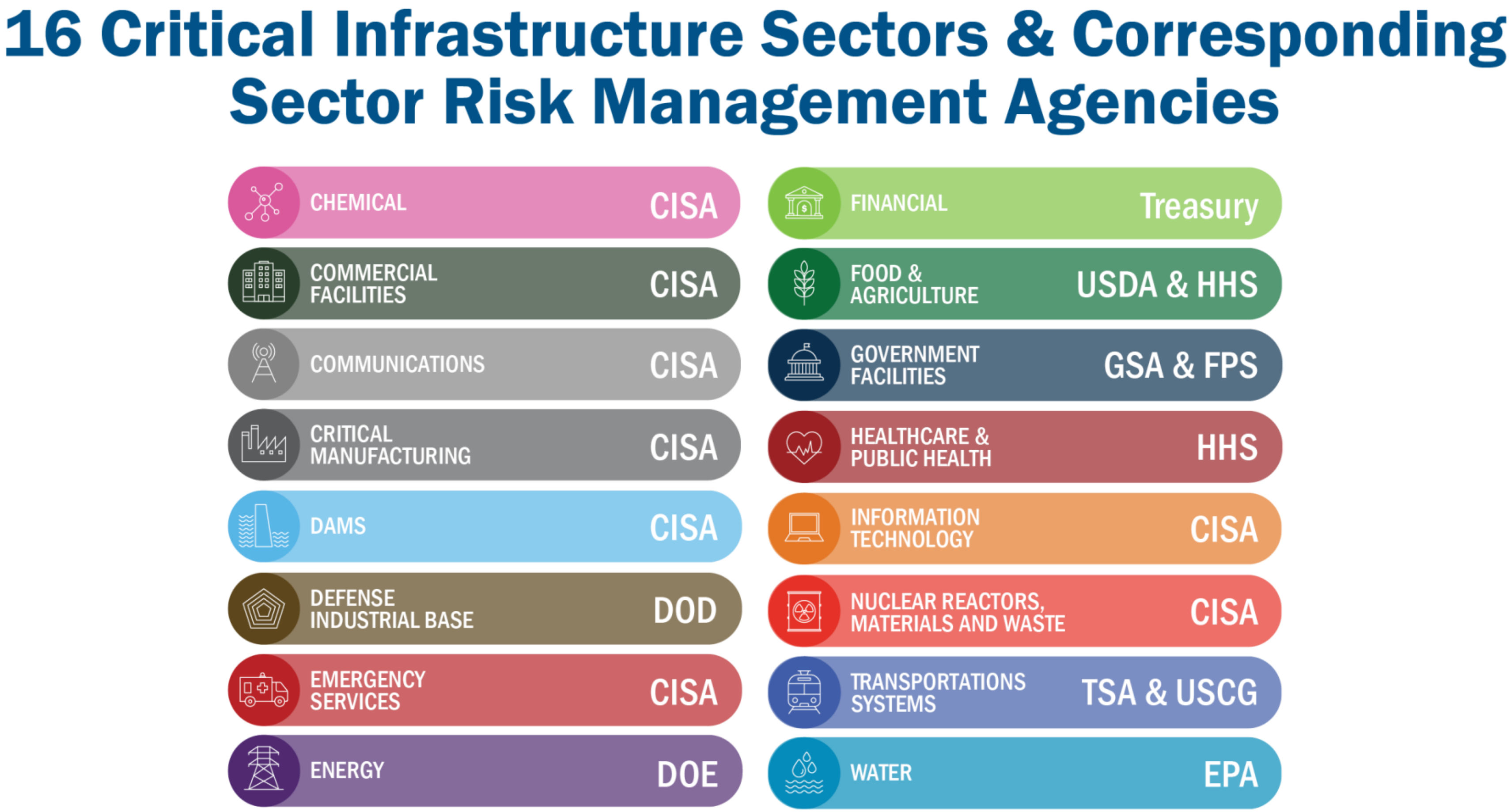
BUILD AND MAINTAIN PARTNERSHIPS

SHARE TIMELY AND ACTIONABLE INFORMATION

COLLABORATE WITH PARTNERS TO MITIGATE RISK

16 CRITICAL INFRASTRUCTURE SECTORS:

16 Critical Infrastructure Sectors



16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

CHEMICAL	CISA
COMMERCIAL FACILITIES	CISA
COMMUNICATIONS	CISA
CRITICAL MANUFACTURING	CISA
DAMS	CISA
DEFENSE INDUSTRIAL BASE	DOD
EMERGENCY SERVICES	CISA
ENERGY	DOE
FINANCIAL	Treasury
FOOD & AGRICULTURE	USDA & HHS
GOVERNMENT FACILITIES	GSA & FPS
HEALTHCARE & PUBLIC HEALTH	HHS
INFORMATION TECHNOLOGY	CISA
NUCLEAR REACTORS, MATERIALS AND WASTE	CISA
TRANSPORTATIONS SYSTEMS	TSA & USCG
WATER	EPA

Regional Team

- Regional Director
- Chief, Protective Security
- **Protective Security Advisor (PSA)**
- Regional PSA (FY19)
- Chief, Chemical Security
- **Chemical Security Inspector (CSI)**
- Senior Chemical Security Inspector
- Regional Operations Manager
- Critical Infrastructure Specialist
- Operations Analyst
- NRMC Regional Analyst
- Regional Regulatory Analyst
- Administrative Officer
- Program Analyst for Business Support
- Outreach Coordinator
- ISC Regional Advisor
- Regional Training & Exercise Coordinator
- Regional Planner (Vacant)
- Soft Target Specialist (Vacant)
- **Cybersecurity Advisor (CSA)**
- **Emergency Communications Coordinator (ECC)**
- **Bombing Prevention Coordinator (BPC)**

Black: Regional Office
Blue: Field

Chemical Security Inspectors

Chemical Security Inspectors visit chemical facilities to ensure that they meet the security requirements set forth by the Chemical Facility Anti-Terrorism Standards (CFATS) Regulatory Security Program. The CFATS program identifies and regulates high-risk Chemical facilities to ensure they have security measures in place to reduce the risk that certain hazardous chemicals are not weaponized by terrorists.

- **Plan, coordinate, and conduct regulatory Inspections and Compliance Assistance Visits**
- **Plan & Conduct Outreach engagement activities**
- **Enforcement Operations**
- **Support Chemical sector security events**

Protective Security Advisors

Protective Security Advisors (PSA) have five mission areas that directly support the protection of critical infrastructure:

- **Plan, coordinate, and conduct security surveys and assessments**
- **Plan and conduct outreach activities**
- **Support National Special Security Events (NSSEs) & Special Event Activity Rating (SEAR) events**
- **Respond to incidents**
- **Coordinate and support improvised explosive device awareness and risk mitigation training**

Cybersecurity Advisors | Introduction

Lead the collaborative national effort to strengthen the security and resilience of America’s critical infrastructure

Cybersecurity Advisors (CSAs) in support of the mission:

- **Assess**: Evaluate critical infrastructure cyber risk.
- **Promote**: Encourage best practices and risk mitigation strategies.
- **Build**: Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate**: Inform and raise awareness.
- **Listen**: Collect stakeholder requirements.
- **Coordinate**: Bring together incident support and lessons learned.

Cybersecurity Advisors | Sampling of Cybersecurity Offerings

- **Preparedness Activities**
  - Information / Threat Indicator Sharing
  - Cybersecurity Training and Awareness
  - Cyber Exercises and “Playbooks”
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices

Cybersecurity Advisors | Sampling of Cybersecurity Offerings

Preparedness Activities

- Range of Cybersecurity Evaluations

Cyber Resilience Review (Strategic)

External Dependencies Management (Strategic)

Cyber Infrastructure Survey (Strategic)

Cybersecurity Evaluations Tool (Standards)

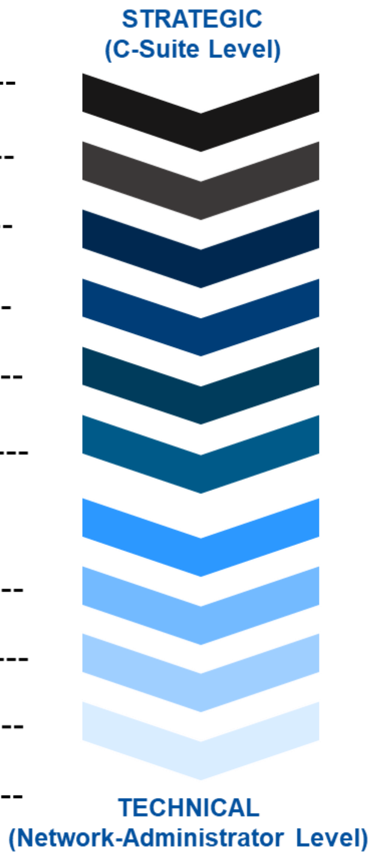
Phishing Campaign Assessment (EVERYONE)

Validated Architecture Design Review (Tactical)

Cyber Hygiene (Technical)

- Vulnerability Scanning
- Web Application Scanning
- Remote Penetration Test

Risk and Vulnerability Assessment (Technical)



Cybersecurity Advisors | Sampling of Cybersecurity Offerings

- **Response Assistance**
  - Remote / On-Site Assistance
  - Malware Analysis
  - Hunt and Incident Response Teams
  - Incident Coordination

Cybersecurity Advisors | Sampling of Cybersecurity Offerings

- **Advisory & Outreach**
  - Working group collaboration
  - Public-private partnership best practices
  - Incident assistance coordination
  - Training / workshops / presentation facilitators

Bomb Prevention Coordinator (BPC) | Region III Pilot

BPC Program Mission

- Analyze state, regional, and local emergency plans for the inclusion of C-IED protocols
- Assess preparedness, mitigation and response capabilities on the state and local levels to identify any gaps that could be filled by a whole of government approach, to include the CISA Bombing Prevention Technical Assistance Program
- Help local jurisdictions build their own BPC positions that could liaison with us to continually manage C-IED efforts

Bomb Prevention Coordinator (BPC) | Region III Pilot

BPC Region III Pilot Overview

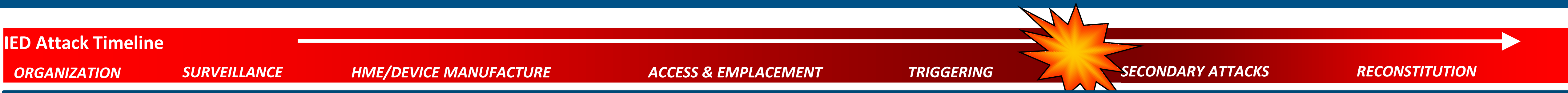
State Level

- Determine if C-IED issues are in the state's Threat Hazard Identification Risk Assessment (THIRA)
- Examine emergency plans
- Assess capabilities with the National Counter-IED Capabilities Analysis Database
- Assess C-IED risk by utilizing Urban Area Security Initiative to focus efforts

Local and Regional

- Develop a plan in coordination with state and local officials in consultation with Region III
- Determine if C-IED issues are on the local and regional THIRA, to examine C-IED plans and assess what capabilities exist at the local and regional level
- Develop and present improvement plans for local and regional jurisdictions

OBP Role in the IED Attack Timeline



IED Attack Timeline

ORGANIZATION *SURVEILLANCE* *HME/DEVICE MANUFACTURE* *ACCESS & EMPLACEMENT* *TRIGGERING* *SECONDARY ATTACKS* *RECONSTITUTION*

Cross-cutting

- TRIPwire and NETF Info/Intel Website and Products
- C-IED Coordination via DHS IED Working Group and JPO C-IED
- C-IED Requirements and Doctrine (SRG for C-IED, and annexes)
- National Counter-IED Capabilities Analysis Database
- Multi-Jurisdiction IED Security Planning
- C-IED Risk Management Training & Guidance Portfolio

Prevention

- Bomb-Making Materials Awareness Program (BMAP) and Op Flashpoint
- National Explosives Task Force
- Surveillance Detection Training & Guidance
- VBIED Detection Training & Guidance

Protection/Mitigation

- Protective Measures Training & Guidance
- RDT&E Requirements
- Explosive Effects Training & Tools
- HME Awareness Training & Guidance
- Bomb-Threat Management Course & Guidance
- Vehicle Inspection Training & Guidance

Response

- IED Search Training & Guidance
- FiRST Smartphone Application
- Response to Suspicious Behaviors/Items Training & Guidance
- Interactive Scenario-based Training for First Responders

The CISA Website

- Excellent site!
  - Cybersecurity
  - Infrastructure Security
  - Emergency Communications
  - National Risk Management
  - Quick Links
  - CISA Services Catalog

CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY

www.CISA.gov
(CISAs main website)

Homeland Security Information Network (HSIN)

HSIN is the trusted network for homeland security mission operations to share sensitive but unclassified information.

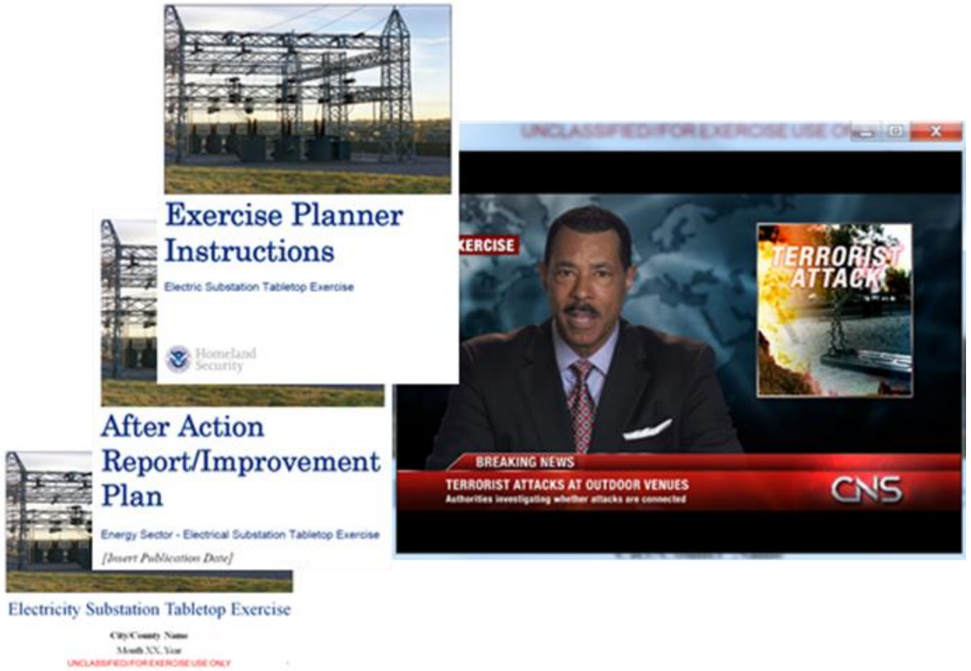
CISA HSIN Communities:

- Critical Infrastructure (HSIN-CI)
- Infrastructure Sectors (16)
- Content Providers
- Resources, including Web Conferencing

https://www.dhs.gov/homeland-security-information-network-hsin

CISA Tabletop Exercise Package (CTEP)

- Each CTEP package contains:
  - A welcome letter
  - Invitation letter
  - Exercise slide deck
  - Situation manuals
  - Facilitator and Evaluator handbook
  - Exercise Planner feedback form
  - Participant feedback form
  - After action report.



Exercise Planner Instructions

Electric Substation Tabletop Exercise

Homeland Security

After Action Report/Improvement Plan

Energy Sector - Electrical Substation Tabletop Exercise

[Insert Publication Date]

Electricity Substation Tabletop Exercise

City/County Name

Month XX, Year

UNCLASSIFIED/FOR EXERCISE USE ONLY

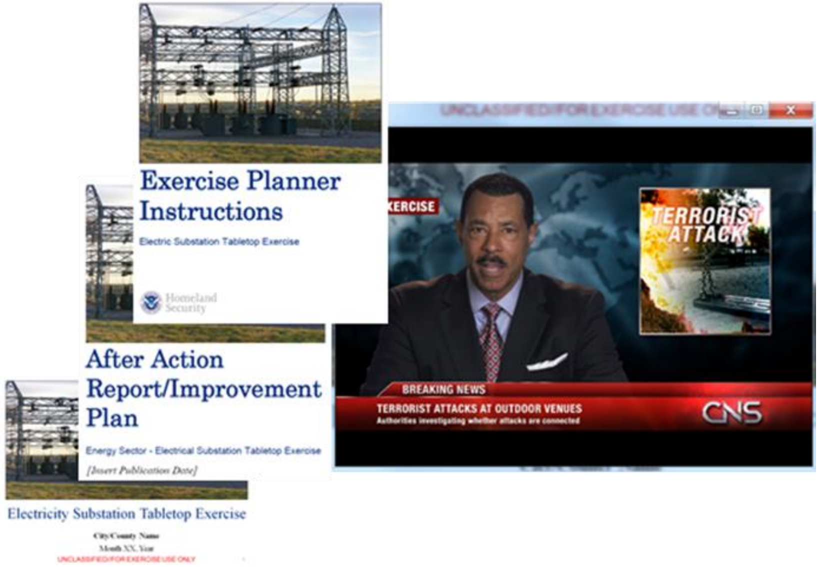
UNCLASSIFIED/FOR EXERCISE USE O
XERCISE
TERRORIST ATTACK
BREAKING NEWS
TERRORIST ATTACKS AT OUTDOOR VENUES
Authorities investigating whether attacks are connected
CNS

https://hsin.dhs.gov/ci/sites/exerciseinfo/Pages/default.aspx

(HSIN-CI Link)

CISA Tabletop Exercise Package (CTEP)

- The exercise planner’s handbook provides systematic instructions on:
  - How to **plan**
  - How to **develop**
  - How to **execute** the tabletop exercise.
- Materials available via Homeland Security Information Network-Critical Infrastructure (HSIN-CI)



Exercise Planner Instructions

Electric Substation Tabletop Exercise

Homeland Security

After Action Report/Improvement Plan

Energy Sector - Electrical Substation Tabletop Exercise

[Insert Publication Date]

Electricity Substation Tabletop Exercise

City/County Name

Month XX, Year

UNCLASSIFIED//FOR EXERCISE USE ONLY

UNCLASSIFIED//FOR EXERCISE USE ON
XERCISE
TERRORIST ATTACK
BREAKING NEWS
TERRORIST ATTACKS AT OUTDOOR VENUES
Authorities investigating whether attacks are connected
CNS

https://hsin.dhs.gov/ci/sites/exerciseinfo/Pages/default.aspx

(HSIN-CI Link)

It all Starts & Ends local…

Homeland Security Starts with Hometown Security

Security starts here.

connect

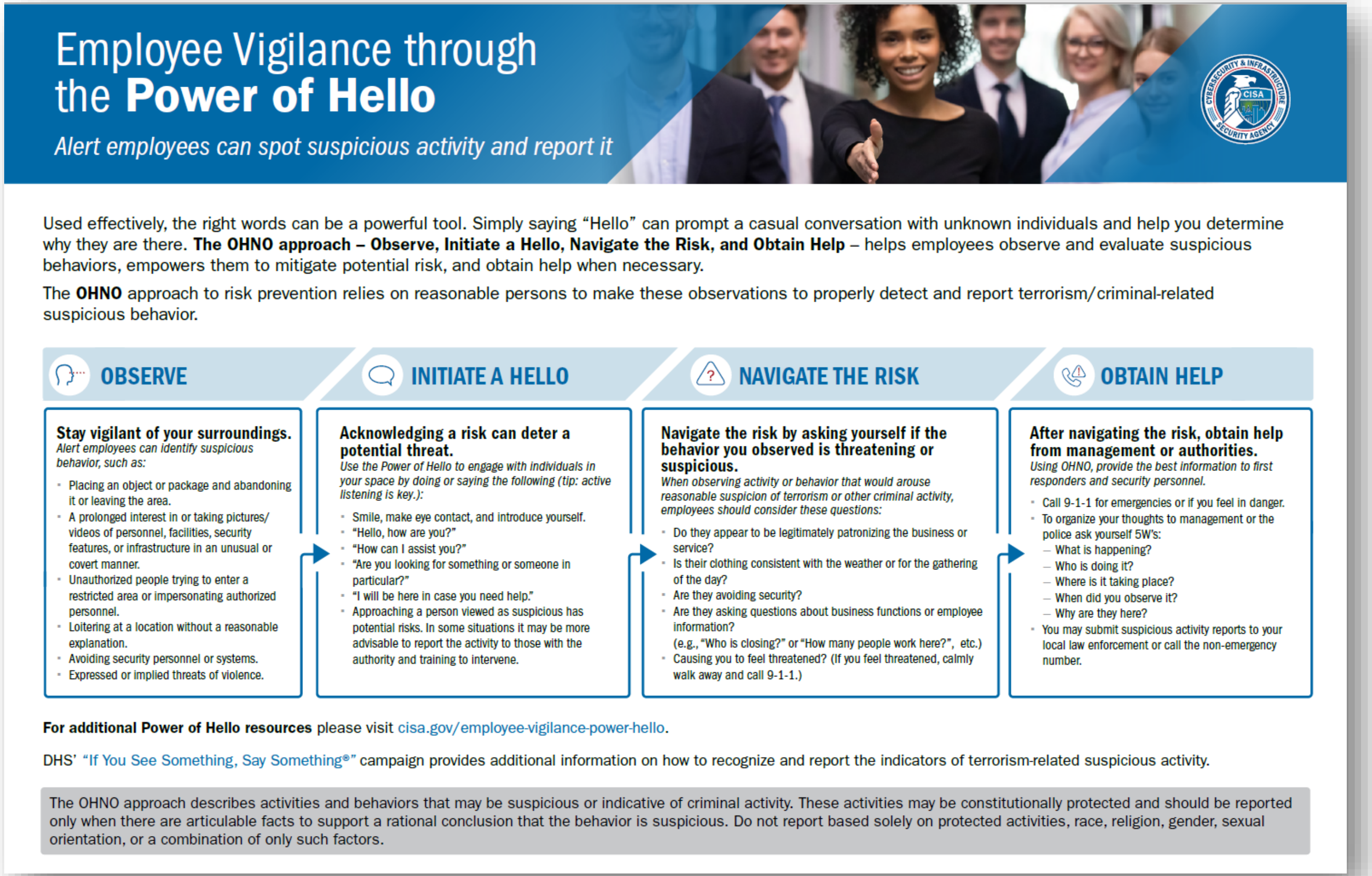
plan

train

report

For more information, visit
www.cisa.gov/hometown-security

Hello...See Something, Say Something



Employee Vigilance through the **Power of Hello**

Alert employees can spot suspicious activity and report it

Used effectively, the right words can be a powerful tool. Simply saying "Hello" can prompt a casual conversation with unknown individuals and help you determine why they are there. **The OHNO approach – Observe, Initiate a Hello, Navigate the Risk, and Obtain Help** – helps employees observe and evaluate suspicious behaviors, empowers them to mitigate potential risk, and obtain help when necessary.

The **OHNO** approach to risk prevention relies on reasonable persons to make these observations to properly detect and report terrorism/criminal-related suspicious behavior.

OBSERVE

Stay vigilant of your surroundings.
Alert employees can identify suspicious behavior, such as:

- Placing an object or package and abandoning it or leaving the area.
- A prolonged interest in or taking pictures/ videos of personnel, facilities, security features, or infrastructure in an unusual or covert manner.
- Unauthorized people trying to enter a restricted area or impersonating authorized personnel.
- Loitering at a location without a reasonable explanation.
- Avoiding security personnel or systems.
- Expressed or implied threats of violence.

INITIATE A HELLO

Acknowledging a risk can deter a potential threat.
Use the Power of Hello to engage with individuals in your space by doing or saying the following (tip: active listening is key.):

- Smile, make eye contact, and introduce yourself.
- "Hello, how are you?"
- "How can I assist you?"
- "Are you looking for something or someone in particular?"
- "I will be here in case you need help."
- Approaching a person viewed as suspicious has potential risks. In some situations it may be more advisable to report the activity to those with the authority and training to intervene.

NAVIGATE THE RISK

Navigate the risk by asking yourself if the behavior you observed is threatening or suspicious.
When observing activity or behavior that would arouse reasonable suspicion of terrorism or other criminal activity, employees should consider these questions:

- Do they appear to be legitimately patronizing the business or service?
- Is their clothing consistent with the weather or for the gathering of the day?
- Are they avoiding security?
- Are they asking questions about business functions or employee information?
  (e.g., "Who is closing?" or "How many people work here?", etc.)
- Causing you to feel threatened? (If you feel threatened, calmly walk away and call 9-1-1.)

OBTAIN HELP

After navigating the risk, obtain help from management or authorities.
Using OHNO, provide the best information to first responders and security personnel.

- Call 9-1-1 for emergencies or if you feel in danger.
- To organize your thoughts to management or the police ask yourself 5W's:
  - What is happening?
  - Who is doing it?
  - Where is it taking place?
  - When did you observe it?
  - Why are they here?
- You may submit suspicious activity reports to your local law enforcement or call the non-emergency number.

For additional Power of Hello resources please visit cisa.gov/employee-vigilance-power-hello.

DHS' "If You See Something, Say Something®" campaign provides additional information on how to recognize and report the indicators of terrorism-related suspicious activity.

The OHNO approach describes activities and behaviors that may be suspicious or indicative of criminal activity. These activities may be constitutionally protected and should be reported only when there are articulable facts to support a rational conclusion that the behavior is suspicious. Do not report based solely on protected activities, race, religion, gender, sexual orientation, or a combination of only such factors.

www.cisa.gov/employee-vigilance-power-hello

Region 3 Contact Information

For questions or requests from specific staff, please reach out to the following:

Resource	Point of Contact
Chemical Security Inspector:	Trevor Cantwell Trevor.Cantwell@hq.dhs.gov 202.805.4957
Protective Security Advisor:	Allen Frenette Allen.Frenette@cisa.dhs.gov 202.836.0750
Cyber Security Advisor:	Jason Schaum Jason.Schaum@cisa.dhs.gov 202.746.2811
Bombing Prevention Coordinator:	Don Grinder Donald.Grinder@cisa.dhs.gov 202.841.3957
Sector Outreach Coordinator:	John French John.French.2@hq.dhs.gov 202.815.9062
Training and Exercise Coordinator:	Joey Whitmoyer Joey.Whitmoyer@hq.dhs.gov 202.815.4592

For more information:
www.cisa.gov

Questions?