

CONSIDERATIONS FOR FACILITY SECURITY BRIEFING

March 2024



Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient
infrastructure for the
American public

MISSION

CISA partners with industry and
government to understand and
manage risk to our Nation's
critical infrastructure.



OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent
threats and hazards

seconds | days | weeks

GOAL 2

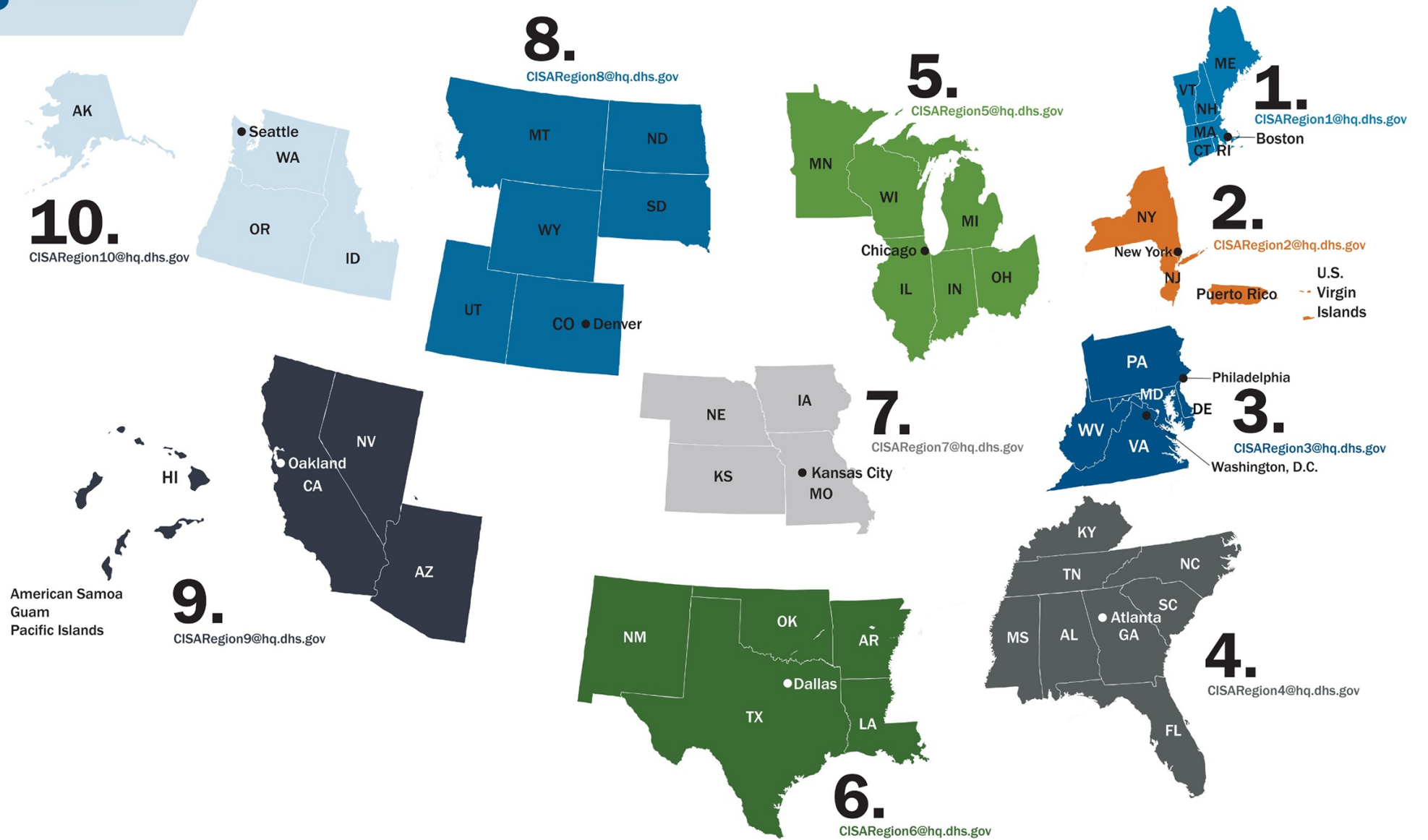
SECURE TOMORROW

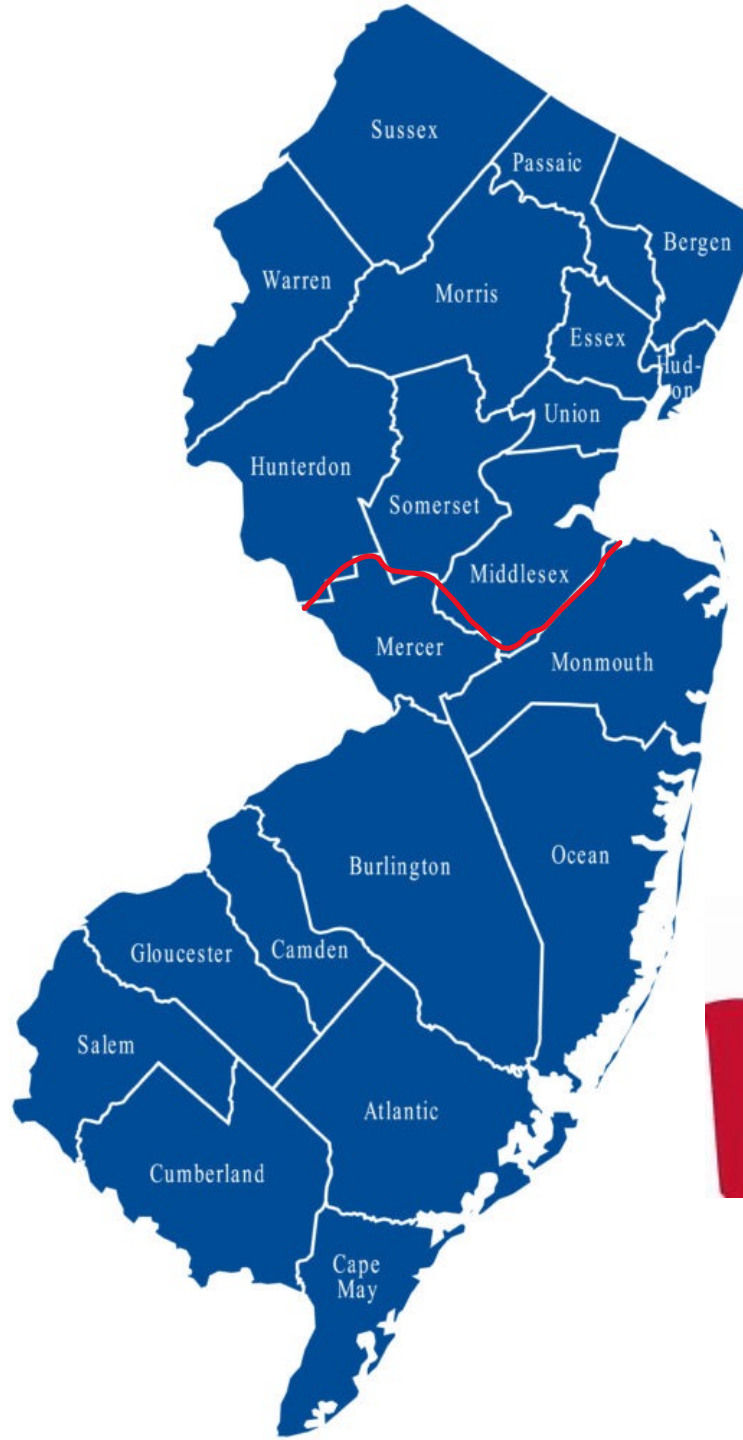
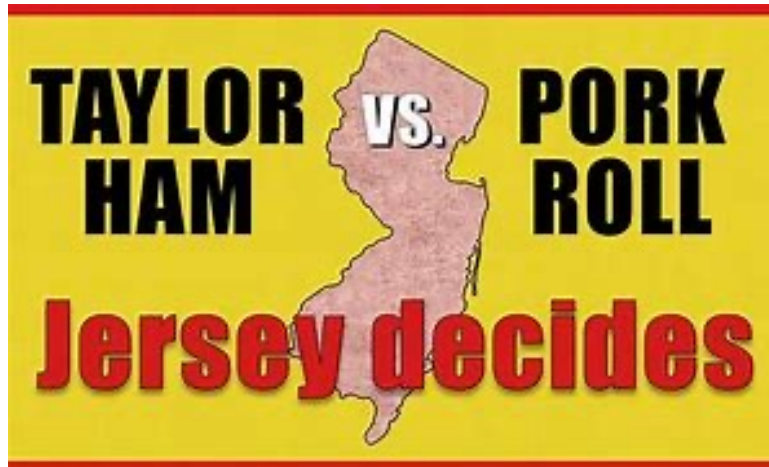
Strengthen critical
infrastructure and
address long-term risks

months | years | decades
















CISA Regions

- 1 Boston, MA
- 2 New York, NY
- 3 Philadelphia, PA
- 4 Atlanta, GA
- 5 Chicago, IL
- 6 Irving, TX
- 7 Kansas City, MO
- 8 Lakewood, CO
- 9 Oakland, CA
- 10 Seattle, WA
- CS Pensacola, FL





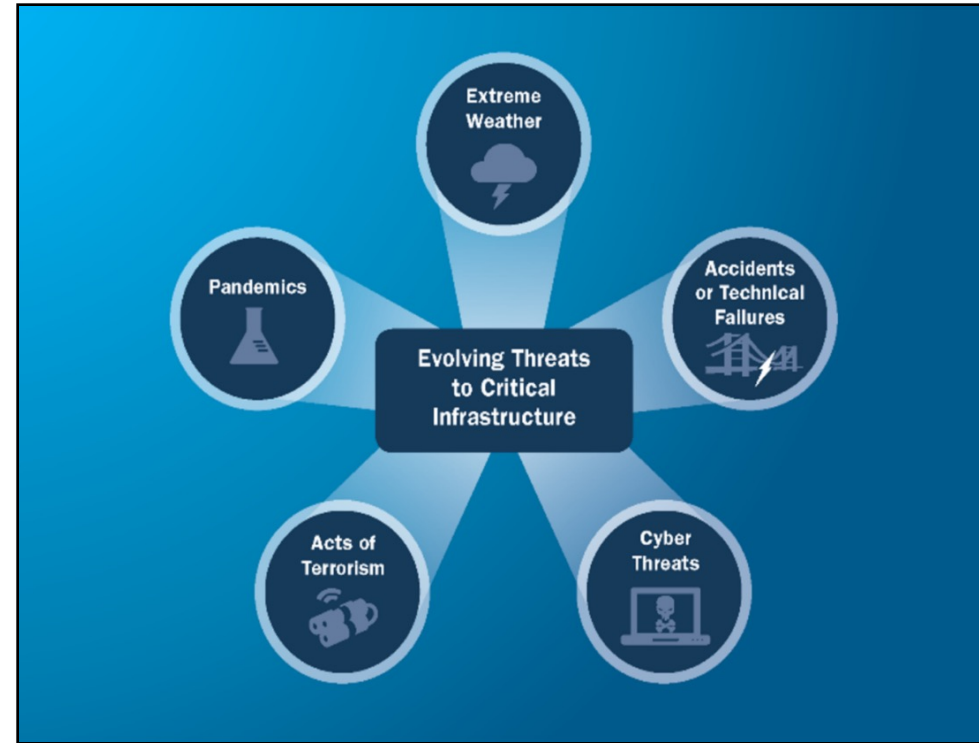
16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

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

Threats to Critical Infrastructure

America remains at risk from a variety of threats including:

- Acts of Terrorism
- Cyber Attacks
- Extreme Weather
- Pandemics
- Accidents or Technical Failures



Threat Vectors



Active Shooter



Vehicle Ramming



Insider Threat

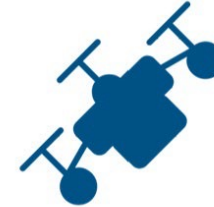


Edged Weapon Attack

Threat Vectors



Improvised Explosive
Device (IED)



Small Unmanned Aircraft
Systems (sUAS)



Fire as a Weapon



Complex Coordinated
Attack (CCA)

Mitigation Options

- Layered Security Approach
- **MULTIPLE MEANS OF PROTECTING YOUR ASSETS**
- Effective security threat mitigation consists of multiple measures designed to safeguard facilities and the public. These mitigation measures can be:
 - Physical
 - Procedural
 - Intelligence-related



Protective Security Advisors

Protective Security Advisors (PSAs) are field-deployed personnel who serve as critical infrastructure security specialists.

We work closely with our local-county and state partners.

UASI Risk Mitigation Planners

County Terrorism Coordinators

NJ Office of Homeland Security and NJ State Police

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



Assist Visits

Establish and enhance DHS's relationship with critical infrastructure owners and operators

Inform them of the importance of their facilities; and reinforce the need for continued vigilance

During an Assist Visit, PSAs focus on coordination, outreach, training, and education

Assist Visits are often followed by security surveys using the Infrastructure Survey Tool (IST) or Security Assessment on First Entry (SAFE) or delivery of other CISA services



SAFE Tool



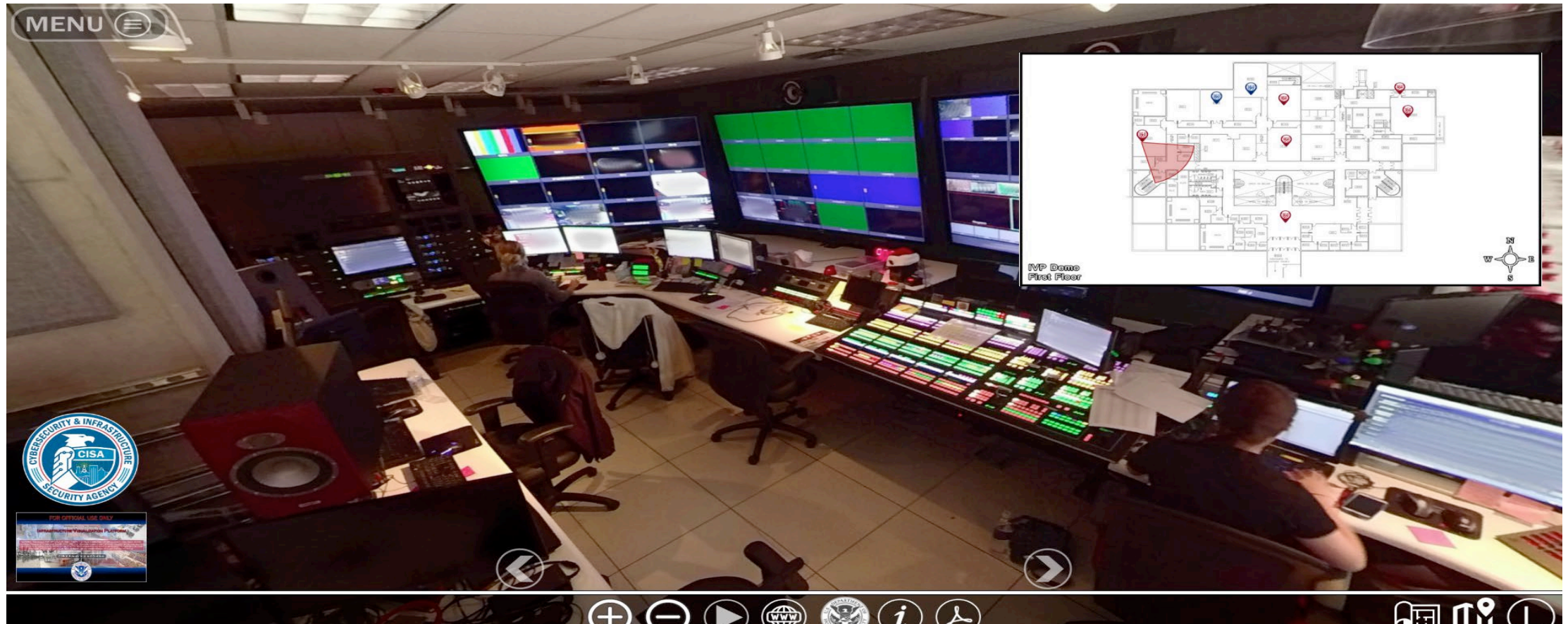
The Security Assessment at First Entry (SAFE) tool is designed to assess the current security posture and identify options for facility owners and operators to mitigate relevant threats

SAFE may be better suited for facilities such as rural county fairgrounds, houses of worship with only weekend services and few members, and small health clinics



Infrastructure Visualization Platform

360 Degree documentation of infrastructure
Command and Control
Emergency Management- Response
Training and Exercise



Infrastructure Survey Tool

The Infrastructure Survey Tool (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



Mitigation Options

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.



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 POWER OF HELLO:

The website corresponding to this QR code is:

cisa.gov/power-hello

"The greatest victory is that which requires no battle." Sun Tzu



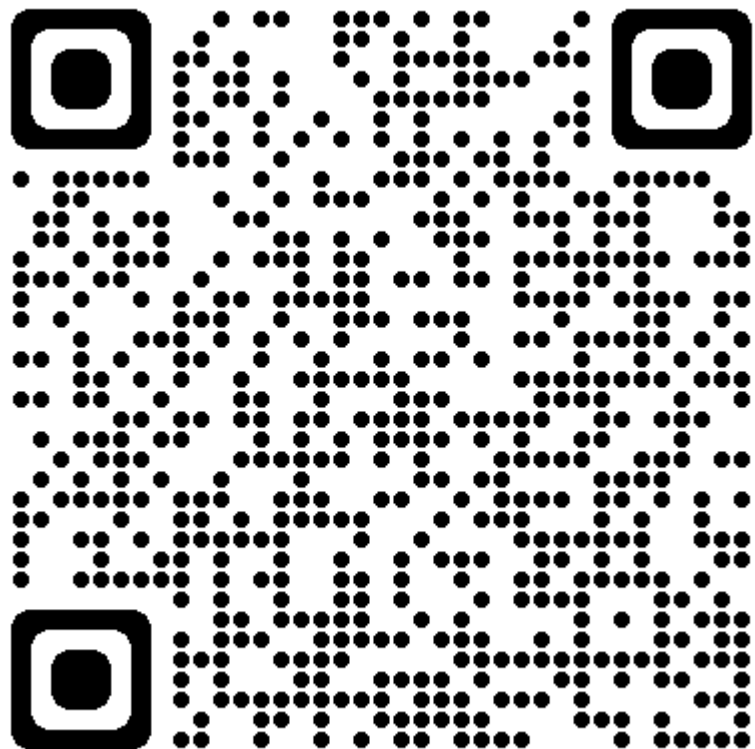
NON-CONFRONTATIONAL TECHNIQUES

The website corresponding to this QR code is:

cisa.gov/topics/physical-security/non-confrontational-techniques

"Build your opponent a golden bridge to retreat across." Sun Tzu





Mitigation Options-NEW



SECURITY PLANNING WORKBOOK

SEPTEMBER 2023

A CONDUCT “AS-IS REVIEW”

Review day-to-day operations, administrative procedures, cybersecurity safeguards, and physical security-related protocols:

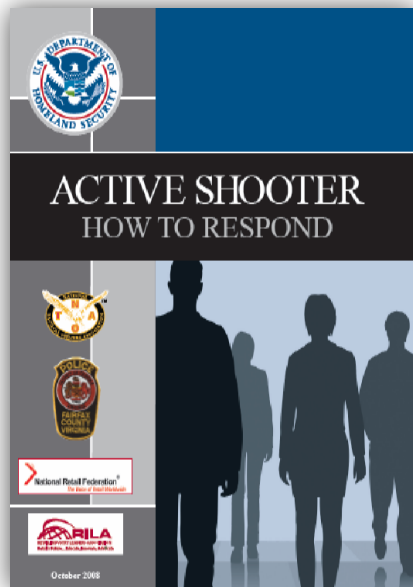
- What are your practices around visitor access?
- What are your hours of operation for your patrons and staff?
- Note which spaces in which areas are routinely kept locked, as well as those routinely unlocked? Should any locks be reassessed?
- Describe the protocol for greeting and screening visitors during events. How does the protocol differ during regular business hours?
- How do you assess compliance with your security policy and procedures? How often do you review and update them?
- Identify how first responders gain access to your facility during an emergency (such as a lockdown situation).

Active Shooter Preparedness

[Businesses & Critical Infrastructure Partners](#)



Active Shooter “How to Respond” Program Overview



To download these materials visit:
[Active Shooter Preparedness | Cybersecurity and Infrastructure Security Agency CISA](#)



RUN-HIDE-FIGHT



PSA Andrew Smith
March 19, 2024

Online Training

DHS released “Active Shooter, What You Can Do” (IS-907), an online training course available through the Federal Emergency Management Agency Emergency Management Institute:

- <http://training.fema.gov/EMIWeb/IS/IS907.asp>

The self-paced course takes approximately 45 minutes to complete.

Upon completion, participants can take a short online "final exam" that is instantly scored. A certificate is provided to participants who finish the course and pass the final exam.



QR Code: FEMA Emergency Management Institute (EMI)

FEMA (FREE) VIRTUAL TRAINING:

<https://training.fema.gov/is/>



QR Code: Active Shooter Preparedness

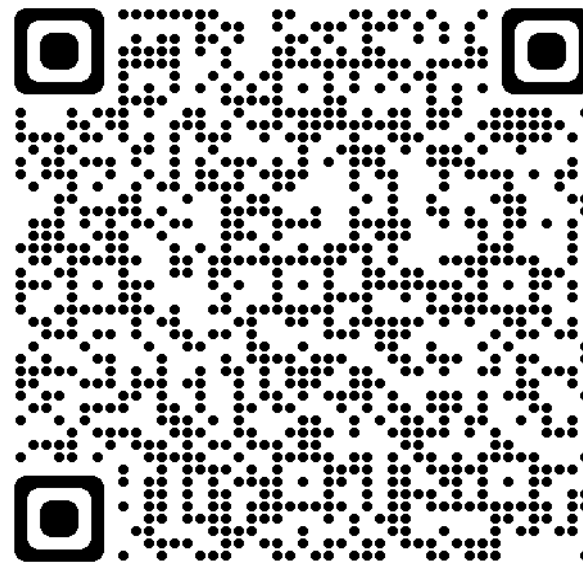
ACTIVE SHOOTER PREPAREDNESS

cisa.gov/topics/physical-security/active-shooter-preparedness



Suspicious Mail or Package Best Practices

To download these materials visit:
<https://www.cisa.gov/publication/isc-mail-handling-non-fou>



Best Practices for Mail Screening and Handling Processes: A Guide for the Public and Private Sectors

September 27, 2012

1st Edition



Homeland Security



Interagency Security Committee

SUSPICIOUS MAIL OR PACKAGES

Protect yourself, your business, and your mailroom.

If you receive a suspicious letter or package:

- Stop. Don't handle.
- Isolate it immediately.
- Don't open, smell, or taste.
- Activate your emergency plan. Notify a supervisor.

The diagram shows a letter and a cardboard box with various red flags labeled:

- Restrictive markings
- No return address
- Sealed with tape
- Misspelled words, badly typed or written
- Unknown powder or suspicious substance
- Possibly mailed from a foreign country
- Excessive postage
- Handwritten "PERSONAL!"
- Postage stamps, discolorations, crystallization on wrapper
- Excessive tape
- Strange odor
- Incorrect size or addressed to S/O only
- Rigid or bulky
- Lopsided or uneven
- Protruding wires

If you suspect the mail or package contains a bomb (explosive), or radiological, biological, or chemical threat:

- Isolate area immediately
- Call 911
- Wash your hands with soap and water

Logos for the U.S. Postal Service and other agencies are at the bottom.

Bomb Threat

BOMB THREAT PROCEDURES

This quick reference checklist is designed to help employees and decision makers of commercial facilities, schools, etc. respond to a bomb threat in an orderly and controlled manner with the first responders and other stakeholders.

Most bomb threats are received by phone. Bomb threats are serious until proven otherwise. Act quickly, but remain calm and obtain information with the checklist on the reverse of this card.

If a bomb threat is received by phone:

1. Remain calm. Keep the caller on the line for as long as possible. DO NOT HANG UP, even if the caller does.
2. Listen carefully. Be polite and show interest.
3. Try to keep the caller talking to learn more information.
4. If possible, write a note to a colleague to call the authorities or, as soon as the caller hangs up, immediately notify them yourself.
5. If your phone has a display, copy the number and/or letters on the window display.
6. Complete the Bomb Threat Checklist immediately. Write down as much detail as you can remember. Try to get exact words.
7. Immediately upon termination of call, DO NOT HANG UP, but from a different phone, contact authorities immediately with information and await instructions.

If a bomb threat is received by handwritten note:

- Call _____
- Handle note as minimally as possible.

If a bomb threat is received by e-mail:

- Call _____
- Do not delete the message.

Signs of a suspicious package:

- No return address
- Excessive postage
- Stains
- Strange odor
- Strange sounds
- Unexpected delivery
- Poorly handwritten
- Misspelled words
- Incorrect titles
- Foreign postage
- Restrictive notes

*** Refer to your local bomb threat emergency response plan for evacuation criteria**

DO NOT:

- Use two-way radios or cellular phone. Radio signals have the potential to detonate a bomb.
- Touch or move a suspicious package.

WHO TO CONTACT (Select One)

- 911
- Follow your local guidelines

For more information about this form contact the DHS Office for Bombing Prevention at OBP@dhs.gov



Homeland Security

2014

BOMB THREAT CHECKLIST

DATE:

TIME:

TIME CALLER HUNG UP:

PHONE NUMBER WHERE CALL RECEIVED:

Ask Caller:

• Where is the bomb located? (building, floor, room, etc.)

• When will it go off?

• What does it look like?

• What kind of bomb is it?

• What will make it explode?

• Did you place the bomb? Yes No

• Why?

• What is your name?

Exact Words of Threat:

Information About Caller:

• Where is the caller located? (background level of noise)

• Estimated age:

• Is voice familiar? If so, who does it sound like?

• Other points:

Caller's Voice

- ☐ Female
- ☐ Male
- ☐ Accent
- ☐ Angry
- ☐ Calm
- ☐ Crying
- ☐ Deep breathing
- ☐ Gravelled
- ☐ Distorted
- ☐ Excited
- ☐ Laughing
- ☐ Liar
- ☐ Loud
- ☐ Nasal
- ☐ Normal
- ☐ Raspy
- ☐ Rapid
- ☐ Raspy
- ☐ Slow
- ☐ Stunned
- ☐ Soft
- ☐ Stutter

Background Sounds

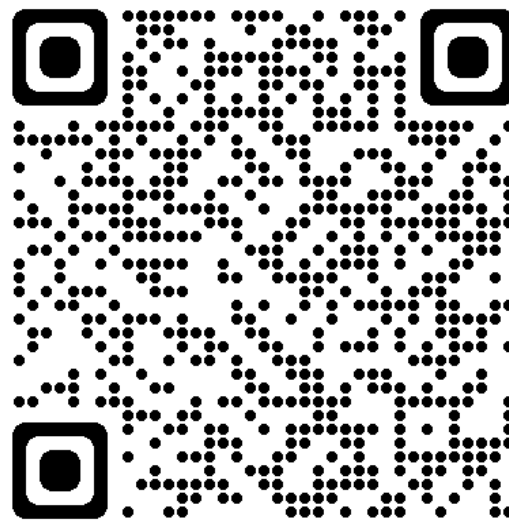
- ☐ Animal noises
- ☐ House noises
- ☐ Kitchen noises
- ☐ Street noises
- ☐ Booth
- ☐ PA system
- ☐ Conversation
- ☐ Music
- ☐ Motor
- ☐ Clear
- ☐ Static
- ☐ Office machinery
- ☐ Factory machinery
- ☐ Local
- ☐ Long Distance

Threat Language

- ☐ Incoherent
- ☐ Message read
- ☐ Taped message
- ☐ Imational
- ☐ Profane
- ☐ Well-spoken

Other Information:

To download these materials visit:
<https://www.cisa.gov/what-to-do-bomb-threat>



BOMB THREAT STAND-OFF CARD



Threat Description	Explosives Capacity	Mandatory Evacuation Distance	Shelter-in-Place Zone	Preferred Evacuation Distance
Pipe Bomb	5 lbs	70 ft	71-1199 ft	+1200 ft
Suicide Bomber	20 lbs	110 ft	111-1699 ft	+1700 ft
Briefcase/Suitcase	50 lbs	150 ft	151-1849 ft	+1850 ft
Car	500 lbs	320 ft	321-1899 ft	+1900 ft
SUV/Van	1,000 lbs	400 ft	401-2399 ft	+2400 ft
Small Delivery Truck	4,000 lbs	640 ft	641-3799 ft	+3800 ft
Container/Water Truck	10,000 lbs	860 ft	861-5099 ft	+5100 ft
Semi-Trailer	60,000 lbs	1570 ft	1571-9299 ft	+9300 ft

CAUTION!

- Do not touch suspicious item
- Notify proper Authorities - Call 911
- Ensure all witnesses are available to brief 1st responders
- Recommended stand-off data should be used in conjunction with your emergency evacuation plan

Preferred Evacuation Distance

Move to Preferred Evacuation Distance. If unable, seek shelter inside of building away from windows and exterior walls.

Shelter-in-Place Zone

Move to Preferred Evacuation Distance. If unable, seek shelter inside of building away from windows and exterior walls.

Mandatory Evacuation Distance

inside and outside of buildings. proceed to Preferred Evacuation Distance

Sources: Department of Homeland Security, Office for Bombing Prevention, Arlington, VA
FBI, Bomb Data Center, Quantico, VA
Technical Support Working Group, Arlington, VA

Mitigation... Next Steps

THE TOP

5

MITIGATIONS
YOU CAN BEGIN
TODAY



1. **Share information** among all possible sources; know your threats.
2. **Create a culture of security awareness** among all employees, volunteers, and willing organizational participants.
3. **Build a team to write and maintain** an Emergency Response Plan AND a Security Plan.
4. **Maintain a purpose-oriented exterior** that enforces boundaries and reduces possible concealment.
5. **Make investments** that improve physical security over time: with detection, preparation, mitigation, and response. *Deter, Detect, Delay, Defend.*

CISA Resources



Active Shooter

- [CISA Active Shooter Preparedness Webpage](#)
- [Employee Vigilance Through the Power of Hello Webpage](#)
- [CISA Faith Based Organizations – Houses of Worship Webpage](#)
- In-Person and Virtual Workshops
- Instructional and Informational Videos
- Action Guides and Fact Sheets
- Posters, Pamphlets, and Pocket Cards



Vehicle Ramming

- [CISA Autonomous Vehicle Security Webpage](#)
- [CISA Vehicle Ramming Attack Mitigation Webpage](#)
- [Vehicle Ramming Action Guide](#)
- [Dams Sector: Active and Passive Vehicle Barriers Guide](#)
- [Autonomous Ground Vehicle Security Guide: Transportation Systems Sector](#)
- [Vehicle Ramming Attack Mitigation Video](#)
- [Guide to Active Vehicle Barrier Specification and Selection Resources](#)
- [Protecting Patrons in Outdoor Eating Venues Fact Sheet](#)



Insider Threat

- [CISA Insider Threat Mitigation Webpage](#)
- [Insider Threat Mitigation Guide](#)
- [Insider Threat 101 Fact Sheet](#)
- [Insider Threat Mitigation Program Fact Sheet](#)
- [Insider Threat Tip Card](#)
- [Insider Risk Mitigation Program Evaluation: Assessment Instrument](#)
- [Understanding Insider Threat Video](#)
- [HR's Role in Preventing Insider Threats Fact Sheet](#)
- [Combating the Insider Threat Advisory](#)
- [NITTF Insider Threat Guide](#)
- [NITTF Maturity Framework\](#)
- [Insider Threat Workshop](#)
- [Insider Threat Workshop One-Pager](#)



CISA Resources, cont'd



Edged Weapon Attacks

- [Mass Gatherings Action Guide](#)
- [Mass Gatherings – Take Charge of Your Personal Safety](#)



Fire as a Weapon

- [Fire as a Weapon Action Guide](#)



Improvised Explosive Devices (IED)

- [CISA Office for Bombing Prevention Webpage](#)
- [What to Do – Bomb Threat Webpage](#)
- [Counter-IED Training Courses](#)
- [Counter-IED Awareness Products](#)
- [Bomb-Making Materials Awareness Program \(BMAP\) Webpage](#)
- [Multi-Jurisdiction Improvised Explosive Device Security Planning \(MJIEDSP\) Webpage](#)
- [National C-IED Capabilities Analysis Database \(NCCAD\) Webpage](#)
- [Security and Resiliency Guide: C-IED Concepts, Common Goals, and Available Assistance](#)
- [Technical Resource for Incident Prevention \(TRIPwire\) Webpage](#)



CISA Resources, cont'd



Complex Coordinated Attack (CCA)

- [Securing Public Gatherings Webpage](#)
- [Mass Gatherings Action Guide](#)
- [Complex Coordinated Attacks Action Guide](#)

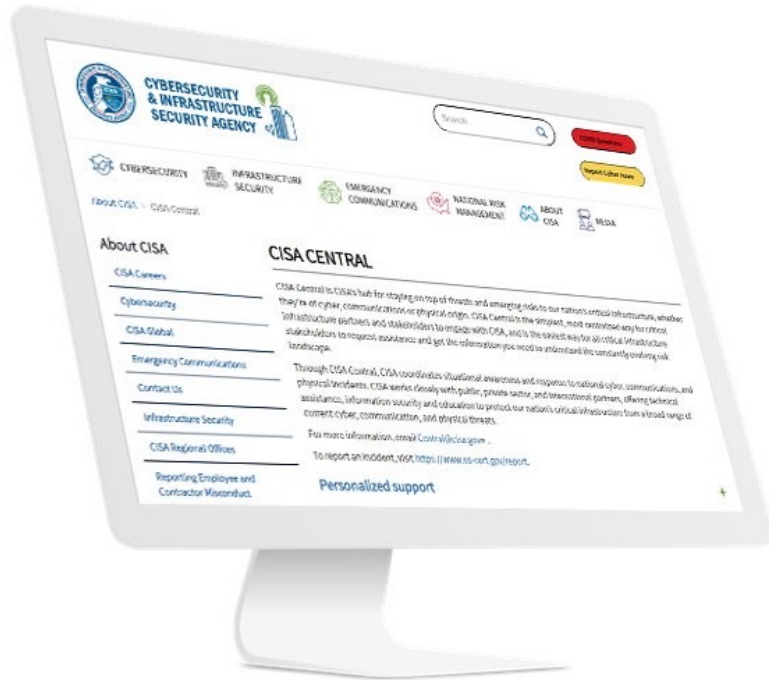


Small Unmanned Aircraft System (sUAS)

- [UAS Webpage](#)
- [UAS and Critical Infrastructure: Understanding the Risk Video](#)
- [sUAS Drone Pocket Card](#)
- [sUAS Security Challenges Fact Sheet/One-Pager](#)
- [Counter UAS Legal Authorities Fact Sheet](#)
- [Recognize Suspicious sUAS Post Card](#)
- [Recognize Suspicious sUAS Poster](#)
- [sUAS Considerations for Law Enforcement Actions](#)
- [UAS FAQs](#)



CISA Can Help!!



cisa.gov/central

CISA and other federal entities provide additional resources to create mitigations for many unique settings.

24/7/365 CONTACT

Contact CISA Central by email, central@cisa.dhs.gov or by phone, [888-282-0870](tel:888-282-0870).



PSA Dan Schultz

CISA NJ-North District-"Sub-Taylor Ham"

“

All NJ counties north of Mercer & Monmouth”

Contact Information:

Dan.Schultz@hq.dhs.gov

202-538-5530

PSA Andrew (Andy) Smith

CISA NJ-South District- “Hoagie-Pork Roll”

Contact Information:

- Andrew.Smith@hq.dhs.gov
- 202-875-1034





For more information:
PSA Andrew (Andy) Smith
Andrew.Smith@hq.dhs.gov
www.cisa.gov

