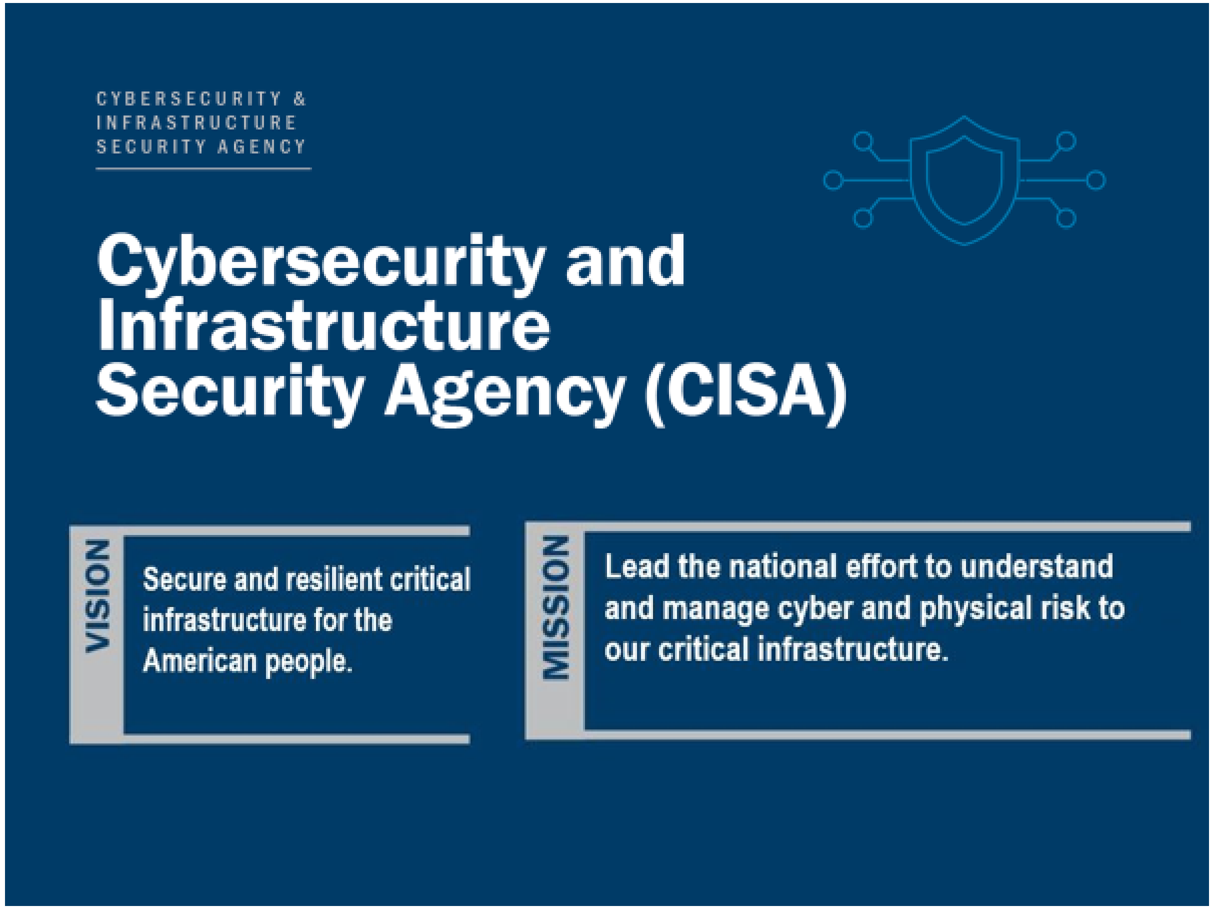
CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

PROTECTIVE SECURITY ADVISOR – ASSIST VISIT

August 16, 2023

Critical Infrastructure Protection



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

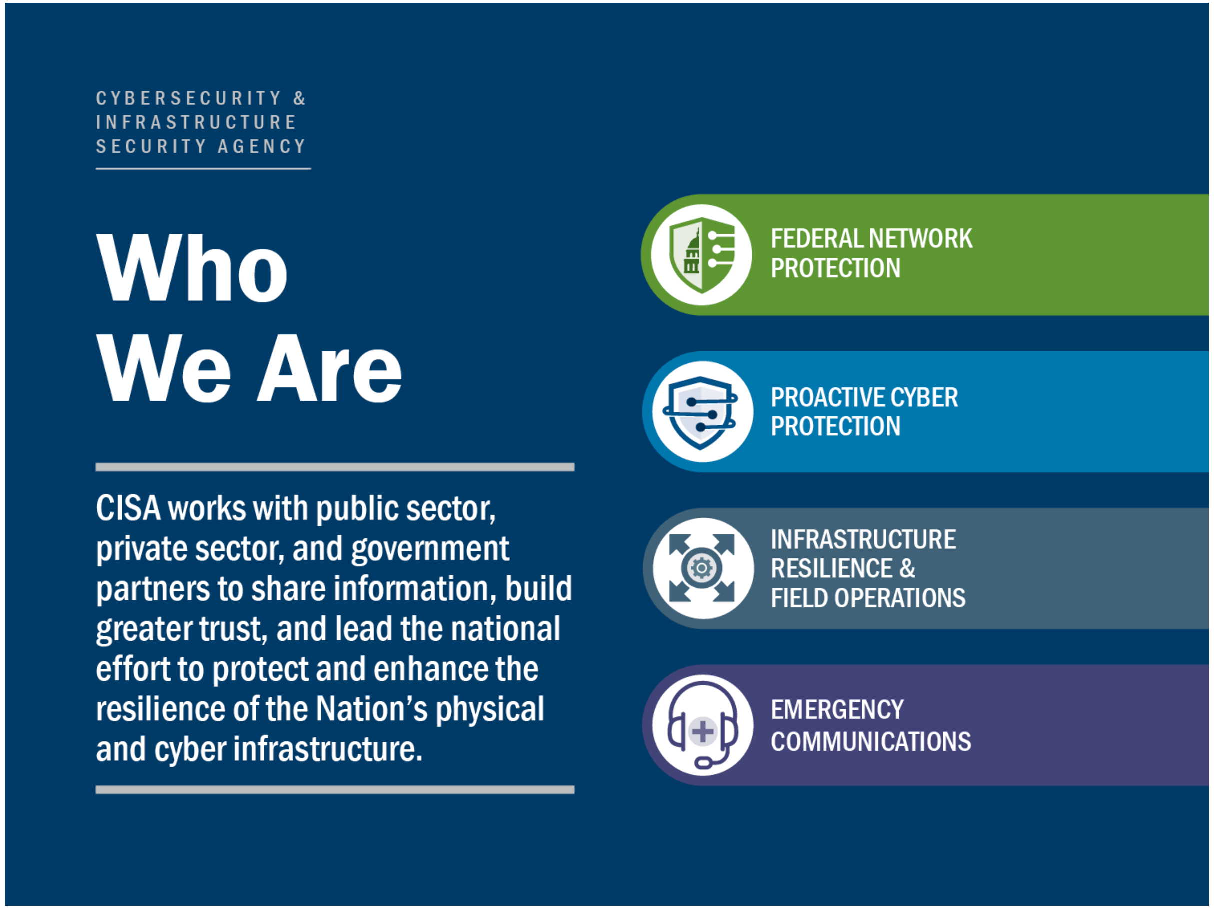
Cybersecurity and Infrastructure Security Agency (CISA)

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.



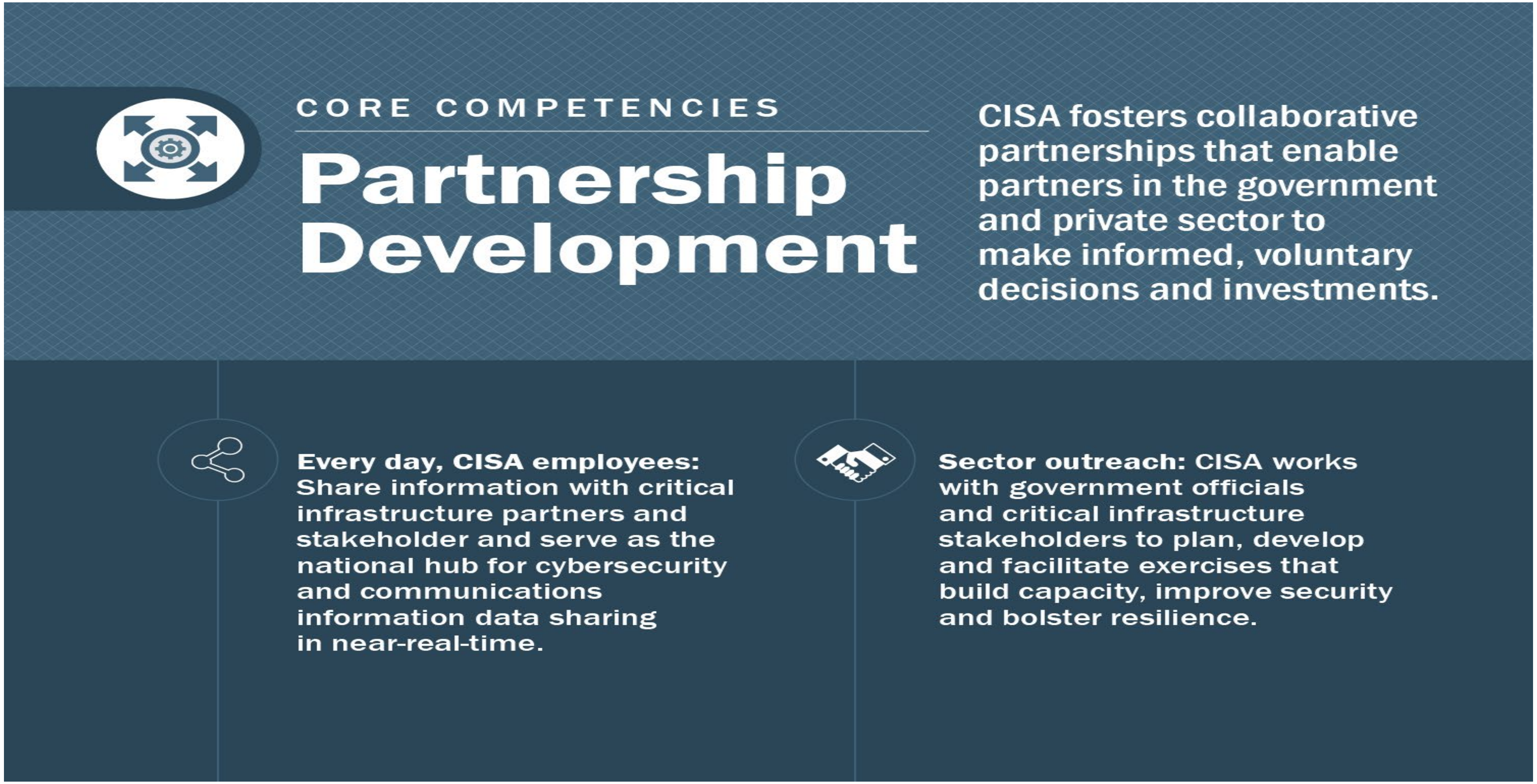
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Who We Are

CISA works with public sector, private sector, and government partners to share information, build greater trust, and lead the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

- FEDERAL NETWORK PROTECTION
- PROACTIVE CYBER PROTECTION
- INFRASTRUCTURE RESILIENCE & FIELD OPERATIONS
- EMERGENCY COMMUNICATIONS

Critical Infrastructure Protection



CORE COMPETENCIES

Partnership Development

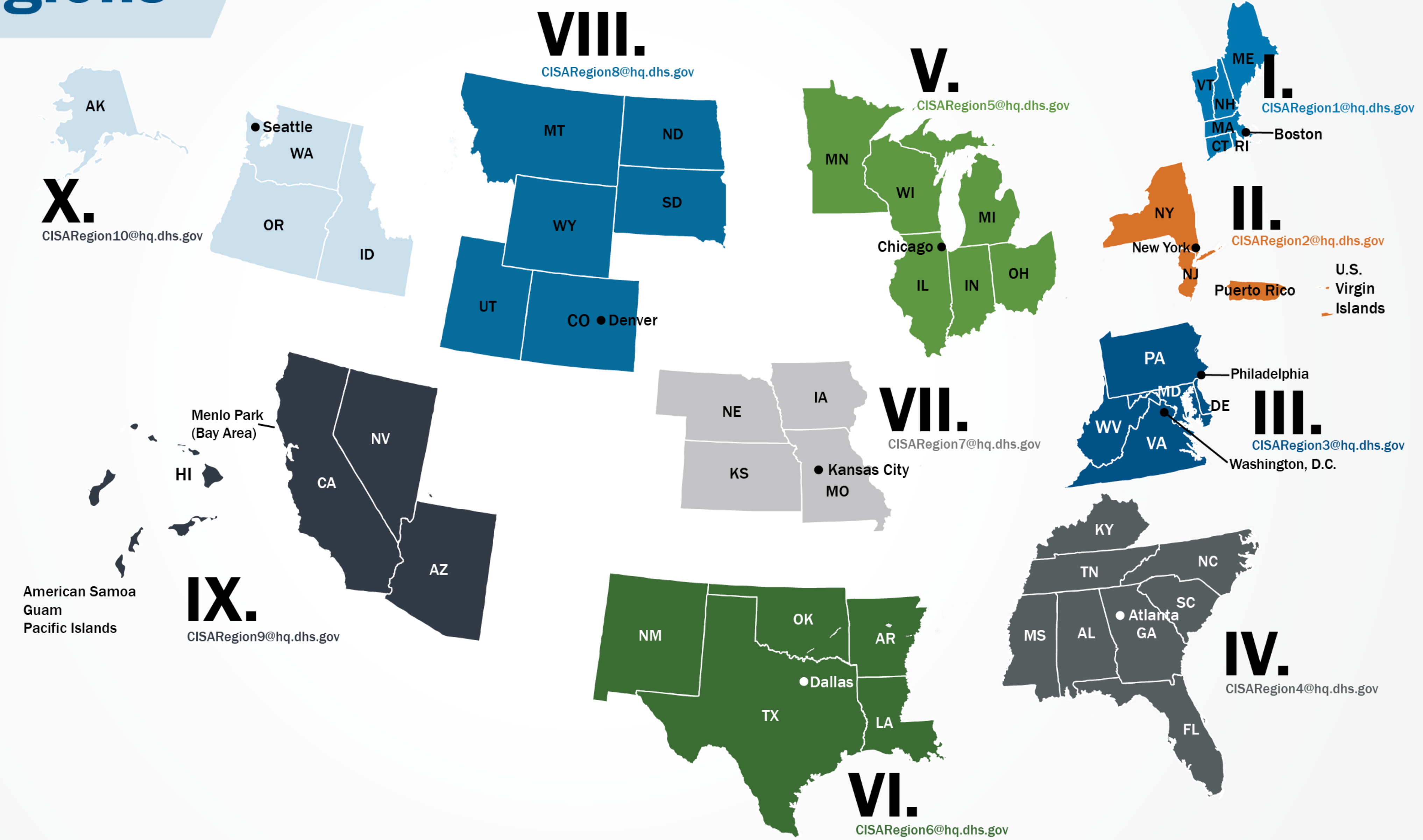
CISA fosters collaborative partnerships that enable partners in the government and private sector to make informed, voluntary decisions and investments.

Every day, CISA employees: Share information with critical infrastructure partners and stakeholder and serve as the national hub for cybersecurity and communications information data sharing in near-real-time.

Sector outreach: CISA works with government officials and critical infrastructure stakeholders to plan, develop and facilitate exercises that build capacity, improve security and bolster resilience.

CISA Regions

I	Boston, MA
II	New York, NY
III	Philadelphia, PA
IV	Atlanta, GA
V	Chicago, IL
VI	Irving, TX
VII	Kansas City, MO
VIII	Lakewood, CO
IX	Oakland, CA
X	Seattle, WA
CS	Pensacola, FL



CISA Region 4

- CISA Region 4, headquartered in Atlanta, Ga., provides cybersecurity and infrastructure security services to six Tribal Nations and the following states:
  - Alabama, Florida, Georgia, Kentucky, Mississippi , North Carolina , South Carolina , Tennessee
- Through our efforts to understand and advise on cyber and physical risks to the nation's critical infrastructure, we help partners strengthen their own capabilities. We connect our stakeholders in industry and government to each other and to resources, analyses, and tools to help them build their own cyber, communications, and physical security and resilience, in turn strengthening national resilience.

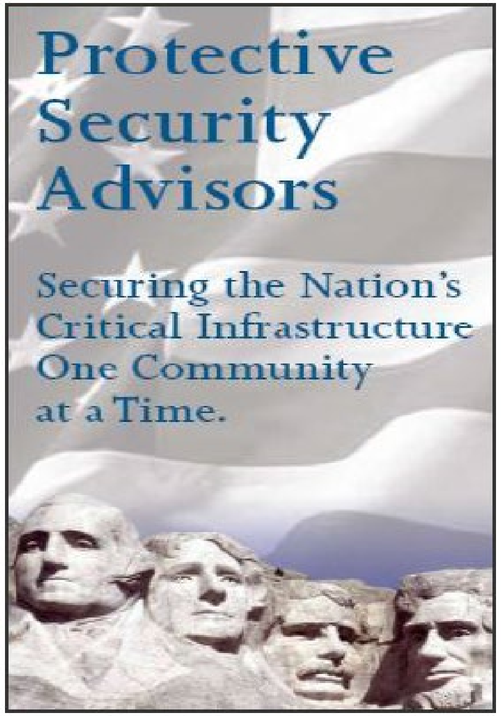
KY
TN
NC
SC
MS
AL
GA
FL

Protective Security Advisors (PSA)

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

- PSAs work with state, local, tribal, territorial (SLTT) and private sector as a link to CISA infrastructure protection resources such as:
  - Security advice
  - Information sharing
  - Incident response
  - Special events
  - Training, exercises and other CISA products and services

- Reach back to DHS / CISA



Protective Security Advisors

Securing the Nation's Critical Infrastructure One Community at a Time.

SAFE Tool

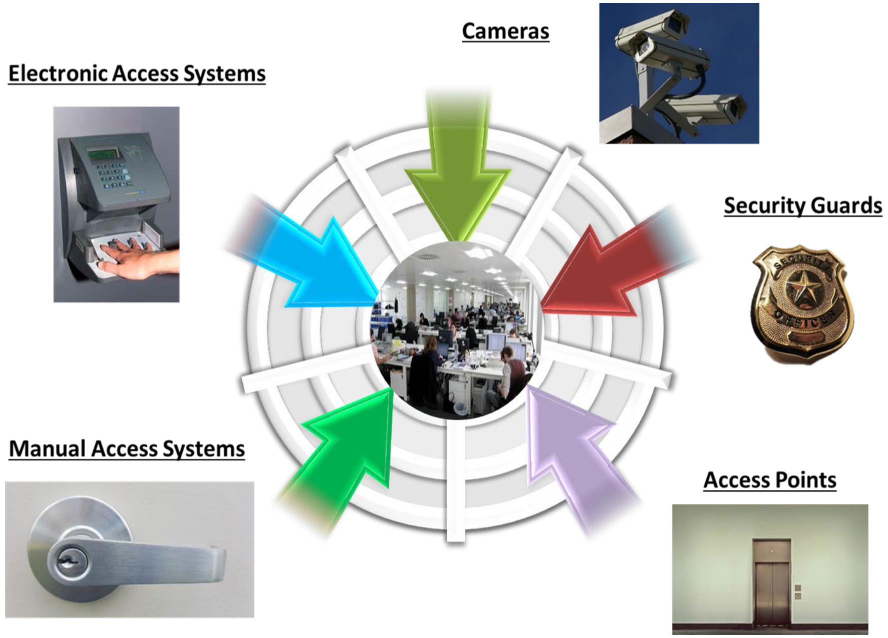
- The Security Assessment at First Entry (SAFE) tool is designed to assess the current security posture and identify options for facility owners and operators to mitigate relevant threats

- The SAFE tool is suited for all facilities, including smaller ones such as rural county fairgrounds, houses of worship with only weekend services and few members, and small health clinics

Common Physical Security Vulnerabilities

Based on activities by CISA Protective Security Advisors:

- Lack of designated security manager.
- No written security, emergency management or business continuity plans.
  - Lack of access control & perimeter security
  - Suspicious package procedures
  - Mass notification procedures
  - Active Shooter procedures
  - Training and exercising
- Lack of alarm and video surveillance systems
- Missed opportunities to collaborate with Law Enforcement and Fusion Centers
- Lack of employee background and recurring checks
- Etc..

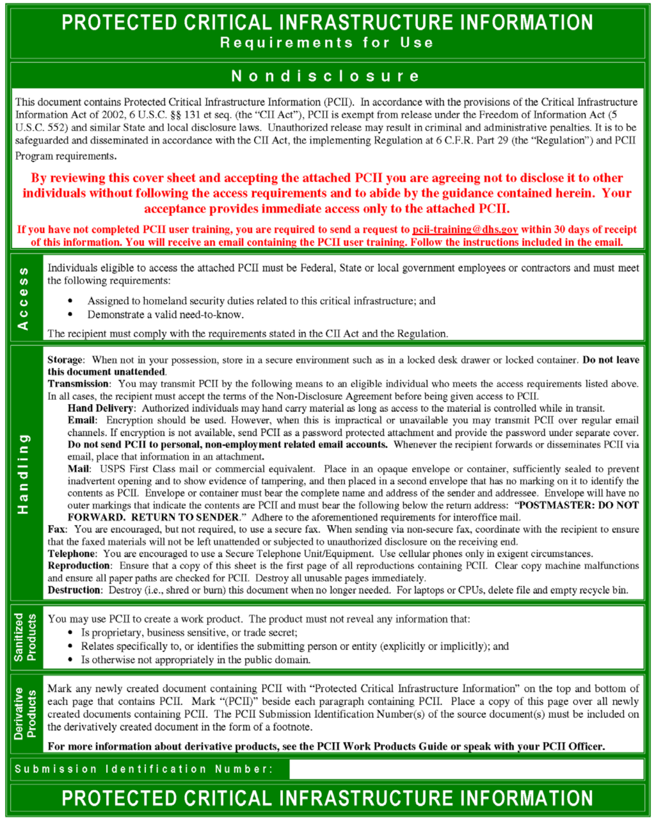


Protected Critical Infrastructure Information

- The Protected Critical Infrastructure Information (PCII) Program protects critical infrastructure information voluntarily shared with the federal government for homeland security purposes
- PCII protects from release through:
  - Freedom of Information Act disclosure requests
  - State, local, tribal, territorial disclosure laws
  - Use in civil litigation
  - Use for regulatory purposes

PCII Protections

- To qualify for PCII protections, information must be related to the security of the critical infrastructure and a submitter must attest the information is:
  - Voluntarily submitted
  - Not customarily found in the public domain
  - Not submitted in lieu of compliance with any regulatory requirement



PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

Requirements for Use

Nondisclosure

This document contains Protected Critical Infrastructure Information (PCII). In accordance with the provisions of the Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 131 et seq. (the "CII Act"), PCII is exempt from release under the Freedom of Information Act (5 U.S.C. 552) and similar State and local disclosure laws. Unauthorized release may result in criminal and administrative penalties. It is to be safeguarded and disseminated in accordance with the CII Act, the implementing Regulation at 6 C.F.R. Part 29 (the "Regulation") and PCII Program requirements.

By reviewing this cover sheet and accepting the attached PCII you are agreeing not to disclose it to other individuals without following the access requirements and to abide by the guidance contained herein. Your acceptance provides immediate access only to the attached PCII.

If you have not completed PCII user training, you are required to send a request to pcii-training@dhs.gov within 30 days of receipt of this information. You will receive an email containing the PCII user training. Follow the instructions included in the email.

Access

Individuals eligible to access the attached PCII must be Federal, State or local government employees or contractors and must meet the following requirements:

- Assigned to homeland security duties related to this critical infrastructure; and
- Demonstrate a valid need-to-know.

The recipient must comply with the requirements stated in the CII Act and the Regulation.

Handling

Storage: When not in your possession, store in a secure environment such as in a locked desk drawer or locked container. **Do not leave this document unattended**.

Transmission: You may transmit PCII by the following means to an eligible individual who meets the access requirements listed above. In all cases, the recipient must accept the terms of the Non-Disclosure Agreement before being given access to PCII.

Hand Delivery: Authorized individuals may hand carry material as long as access to the material is controlled while in transit.

Email: Encryption should be used. However, when this is impractical or unavailable you may transmit PCII over regular email channels. If encryption is not available, send PCII as a password protected attachment and provide the password under separate cover. **Do not send PCII to personal, non-employment related email accounts.** Whenever the recipient forwards or disseminates PCII via email, place that information in an attachment.

Mail: USPS First Class mail or commercial equivalent. Place in an opaque envelope or container, sufficiently sealed to prevent inadvertent opening and to show evidence of tampering, and then placed in a second envelope that has no marking on it to identify the contents as PCII. Envelope or container must bear the complete name and address of the sender and addressee. Envelope will have no outer markings that indicate the contents are PCII and must bear the following below the return address: "**POSTMASTER: DO NOT FORWARD. RETURN TO SENDER**." Adhere to the aforementioned requirements for interoffice mail.

Fax: You are encouraged, but not required, to use a secure fax. When sending via non-secure fax, coordinate with the recipient to ensure that the faxed materials will not be left unattended or subjected to unauthorized disclosure on the receiving end.

Telephone: You are encouraged to use a Secure Telephone Unit/Equipment. Use cellular phones only in exigent circumstances.

Reproduction: Ensure that a copy of this sheet is the first page of all reproductions containing PCII. Clear copy machine malfunctions and ensure all paper paths are checked for PCII. Destroy all unusable pages immediately.

Destruction: Destroy (i.e., shred or burn) this document when no longer needed. For laptops or CPUs, delete file and empty recycle bin.

Sanitized Products

You may use PCII to create a work product. The product must not reveal any information that:

- Is proprietary, business sensitive, or trade secret;
- Relates specifically to, or identifies the submitting person or entity (explicitly or implicitly); and
- Is otherwise not appropriately in the public domain.

Derivative Products

Mark any newly created document containing PCII with "Protected Critical Infrastructure Information" on the top and bottom of each page that contains PCII. Mark "(PCII)" beside each paragraph containing PCII. Place a copy of this page over all newly created documents containing PCII. The PCII Submission Identification Number(s) of the source document(s) must be included on the derivatively created document in the form of a footnote.

For more information about derivative products, see the PCII Work Products Guide or speak with your PCII Officer.

Submission Identification Number:

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

Securing Public Gatherings

Today's dynamic threat environment poses unique risks to infrastructure, particularly to those open to the public

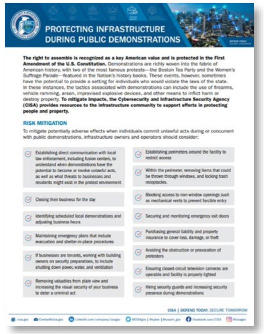
Active Shooter Preparedness and Security Program
Directly and tangibly supports public and private sector stakeholders in enhancing risk mitigation capabilities against the active shooter threat, the most prominent attack vector in the U.S.

Insider Threat Mitigation
Develops and maintains public facing resources to support organizations in creating or improving an insider threat mitigation program to mitigate insider threats.

Vehicle Ramming Mitigation
Provides expertise and guidance to assist SLTT and private sector partners mitigate vehicle ramming threats.

Countering Improvised Explosive Devices (IEDs)
Educates on strategies to prevent, protect against, respond to, and mitigate bombing incidents.

Protecting Infrastructure During Public Demonstrations



PROTECTING INFRASTRUCTURE DURING PUBLIC DEMONSTRATIONS

The right to assemble is recognized as a key American value and is protected in the First Amendment of the U.S. Constitution. Demonstrations are richly woven into the fabric of American history, with two of the most famous protests—the Boston Tea Party and the Women's Suffrage Parade—featured in the Nation's history books. These events, however, sometimes have the potential to provide a setting for individuals who would violate the laws of the state. In these instances, the tactics associated with demonstrations can include the use of firearms, vehicle ramming, arson, improvised explosive devices, and other means to inflict harm or destroy property. **To mitigate impacts, the Cybersecurity and Infrastructure Security Agency (CISA) provides resources to the infrastructure community to support efforts in protecting people and property.**

RISK MITIGATION

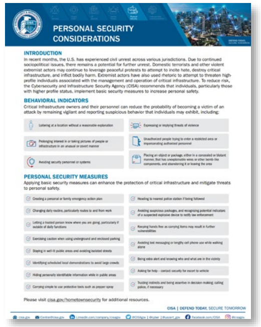
To mitigate potentially adverse effects when individuals commit unlawful acts during or concurrent with public demonstrations, infrastructure owners and operators should consider:

- ✓ Establishing direct communication with local law enforcement, including fusion centers, to understand when demonstrations have the potential to become or involve unlawful acts, as well as what threats to businesses and residents might exist in the protest environment
- ✓ Closing their business for the day
- ✓ Identifying scheduled local demonstrations and adjusting business hours
- ✓ Maintaining emergency plans that include evacuation and shelter-in-place procedures
- ✓ If businesses are tenants, working with building owners on security preparations, to include shutting down power, water, and ventilation
- ✓ Removing valuables from plain view and increasing the visual security of your business to deter a criminal act
- ✓ Establishing perimeters around the facility to restrict access
- ✓ Within the perimeter, removing items that could be thrown through windows, and locking trash receptacles.
- ✓ Blocking access to non-window openings such as mechanical vents to prevent forcible entry
- ✓ Securing and monitoring emergency exit doors
- ✓ Purchasing general liability and property insurance to cover loss, damage, or theft
- ✓ Avoiding the obstruction or provocation of protesters
- ✓ Ensuring closed-circuit television cameras are operable and facility is properly lighted
- ✓ Hiring security guards and increasing security presence during demonstrations

CISA | DEFEND TODAY, SECURE TOMORROW

cisa.gov | Central@cisa.gov | Linkedin.com/company/cisagov | @CISAgov | @cyber | @uscert_gov | Facebook.com/CISA | @cisagov

Personal Security Considerations



PERSONAL SECURITY CONSIDERATIONS

INTRODUCTION

In recent months, the U.S. has experienced civil unrest across various jurisdictions. Due to continued sociopolitical issues, there remains a potential for further unrest. Domestic terrorists and other violent extremist actors may continue to leverage peaceful protests to attempt to incite hate, destroy critical infrastructure, and inflict bodily harm. Extremist actors have also used rhetoric to attempt to threaten high-profile individuals associated with the management and operation of critical infrastructure. To reduce risk, the Cybersecurity and Infrastructure Security Agency (CISA) recommends that individuals, particularly those with higher profile status, implement basic security measures to increase personal safety.

BEHAVIORAL INDICATORS

Critical Infrastructure owners and their personnel can reduce the probability of becoming a victim of an attack by remaining vigilant and reporting suspicious behavior that individuals may exhibit, including:

- Loitering at a location without a reasonable explanation
- Prolonging interest in or taking pictures of people or infrastructure in an unusual or covert manner
- Avoiding security personnel or systems
- Expressing or implying threats of violence
- Unauthorized people trying to enter a restricted area or impersonating authorized personnel
- Placing an object or package, either in a concealed or blatant manner, that has unexplainable wires or other bomb-like components, and abandoning it or leaving the area

PERSONAL SECURITY MEASURES

Applying basic security measures can enhance the protection of critical infrastructure and mitigate threats to personal safety.

- ✓ Creating a personal or family emergency action plan
- ✓ Changing daily routine, particularly routes to and from work
- ✓ Letting a trusted person know where you are going, particularly if outside of daily functions
- ✓ Exercising caution when using underground and enclosed parking
- ✓ Staying in well-lit public areas and avoiding isolated streets
- ✓ Identifying scheduled local demonstrations to avoid large crowds
- ✓ Hiding personally identifiable information while in public areas
- ✓ Carrying simple to use protective tools such as pepper spray
- ✓ Heading to nearest police station if being followed
- ✓ Avoiding suspicious packages, and recognizing potential indicators of a suspected explosive device to notify law enforcement
- ✓ Keeping hands free as carrying items may result in further vulnerabilities
- ✓ Avoiding text messaging or lengthy cell phone use while walking alone
- ✓ Being extra alert and knowing who and what are in the vicinity
- ✓ Asking for help – contact security for escort to vehicle
- ✓ Trusting instincts and being assertive in decision-making; calling police, if necessary

Please visit cisa.gov/hometownsecurity for additional resources.

CISA | DEFEND TODAY, SECURE TOMORROW

cisa.gov | Central@cisa.gov | Linkedin.com/company/cisagov | @CISAgov | @cyber | @uscert_gov | Facebook.com/CISA | @cisagov

Employee Vigilance Through the Power of Hello

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

INITIATE A HELLO
Acknowledging a risk can deter a potential threat

NAVIGATE THE RISK
Determine if the behavior you observed is threatening or suspicious

OBTAIN HELP
Obtain help from management or authorities

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.

Unauthorized Drones over Stadiums

UNAUTHORIZED DRONE ACTIVITY OVER SPORTING VENUES

OVERVIEW

Many professional sporting events are restricting fans from their venues in response to state ordinances that limit public gatherings during the COVID-19 pandemic. Recent drone sightings prompted game delays at sporting venues in Minneapolis, Boston, Los Angeles, Chicago, and New York City, highlighting concerns of unauthorized drone activity in the new spectator-restricted environment. Most instances involve fans seeking real-time game footage. However, malicious actors may utilize drones to disrupt, harass, or even cause physical injury or destruction of property. Regardless of intent, unauthorized drone activities pose a potential risk. Sporting venue owners and operators should therefore consider all unauthorized drone activity with caution and plan accordingly.

This resource presents options of consideration for sporting venue owners and operators to prevent, protect from, and respond to unauthorized drone activity.

PREVENT

Clear and consistent communication with your community is vital to preventing unauthorized drone activity around a venue. Members of the community may include, but are not limited to, residents, businesses, fans, and local law enforcement. Consider the following actions when communicating with stakeholders.

Engage with law enforcement. Connect with federal, state, and local law enforcement early, including the Federal Bureau of Investigation (FBI) and Federal Aviation Administration (FAA) Law Enforcement Assistance Program (LEAP).[1] Notify them of upcoming events and associated risks. Ask about available tools and resources (messaging, technological systems, etc.), and work together to develop a protection and response plan.

Connect with the local Protective Security Advisor (PSA). Cybersecurity and Infrastructure Security Agency (CISA) PSAs are critical infrastructure protection and vulnerability mitigation experts located across the country to conduct assessments, deliver training, and advise on effective ways to enhance security.[2]

Promote public awareness. Use social media, television and radio commercial spots, and outreach to local drone user groups, as well as event goers (and fans), to raise public awareness of flight restrictions and how to report unauthorized flight activity.

Post signage. Identify potential drone launch points around the venue and post signage that designates these areas as "no drone zones." The FAA's free digital toolkit includes No Drone Zone signage for print and web.[3]

Review laws and regulations. Determine whether your facility is covered under 14 CFR 99.7, Special Security Instructions, which restricts unauthorized drone operations one hour before and one hour after certain events at stadiums with a seating capacity of 30,000 or more.[4] Additional regulatory options may include:

- **Temporary Flight Restrictions (TFRs):** TFRs are a type of Notices to Airmen (NOTAM), issued by the FAA, that define an area restricted to air travel due to a hazardous condition, a special event, or a general warning for the entire airspace under their authority.[5] Although a TFR will not counter a drone incursion, it will provide law enforcement the ability to enforce federally mandated flight restrictions. A TFR violation may result in civil penalties and criminal charges.[6] PSAs can assist owners and operators in requesting TFRs for events with a credible drone threat.
- **State and local statutes:** Review state laws, local ordinances/limitations, and private property policies. Laws regarding reckless endangerment, disturbing the peace, and voyeurism may apply to unauthorized drone activity.[7] Incorporate this information into a protection plan and communicate the potential consequences of unauthorized drone activity to the public.

[1] For a list of FBI field offices, visit https://www.fbi.gov/contact-us/field-offices/; for more information about FAA's LEAP visit [illegible]
[2] To learn more about PSAs, visit cisa.gov/protective-security-advisors or send an email to Central@cisa.gov.
[3] "No Drone Zone," FAA, last modified August 2019, [illegible]
[4] Refer to the full NOTAM here: [illegible] and connect with federal, state, and local law enforcement to discuss enforcement options.
[5] To learn more about TFRs, visit [illegible]
[6] For more information about FBI's potential criminal enforcement actions for violations of national defense airspace, refer to 14 CFR 99.7 and 49 U.S. Code § 46307.
[7] To learn more about state drone laws, visit [illegible]

CISA | DEFEND TODAY, SECURE TOMORROW

cisa.gov | Central@cisa.gov | Linkedin.com/company/cisagov | @CISAgov | @cyber | @uscert_gov | Facebook.com/CISA | @cisagov

De-Escalation Series

DE-ESCALATION SERIES FOR CRITICAL INFRASTRUCTURE OWNERS AND OPERATORS

DE-ESCALATION

How You Can Help Defuse Potentially Violent Situations

De-Escalation

"The use of communication or other techniques during an encounter to stabilize, slow, or reduce the intensity of a potentially violent situation without using physical force, or with a reduction in force."

– Department of Homeland Security Policy Statement 044-05

De-Escalation is a method to prevent potential violence. Individuals are encouraged to use purposeful actions, verbal communications, and body language to calm a potentially dangerous situation.

Your safety and the safety of others is the highest priority. Maintain a safe distance and avoid being alone with an individual who is combative or potentially violent. If there is a risk of imminent violence, remove yourself from the situation and seek safety.

Know your limits. Keep in mind that some individuals may be more adept in applying these techniques. Know your own vulnerabilities and tendencies and recognize that sometimes the best intervention is knowing when to seek additional help.

Obtain Help. If you feel the individual or situation is escalating and violence may occur, call for help from your security staff or local law enforcement and move yourself to a safe location.

TIPS

- Be aware of your non-verbal communications. Ensure your tone, facial expressions, body language, and gestures relay calm and empathy.
- Remain respectful and courteous. Address the individual with civility and use phrases such as "please" and "thank you."

This document describes activities and behaviors that may be concerning or indicative of impending violence. Some of these activities while concerning, may be constitutionally protected and should be reported only when there are sufficient facts to support a rational conclusion that the behavior represents a potential threat of violence. Do not report based solely on protected activities, or on the basis of race, religion, gender, sexual orientation, age, disability, or a combination of only such factors. In addition, be aware that critical infrastructure owners and their operations may also be targeted based on these factors.

cisa.gov/securing-public-gatherings

Office for Bombing Prevention (OBP)

CISA OBP accomplishes its mission through a portfolio of complementary counter-IED (C-IED) services.

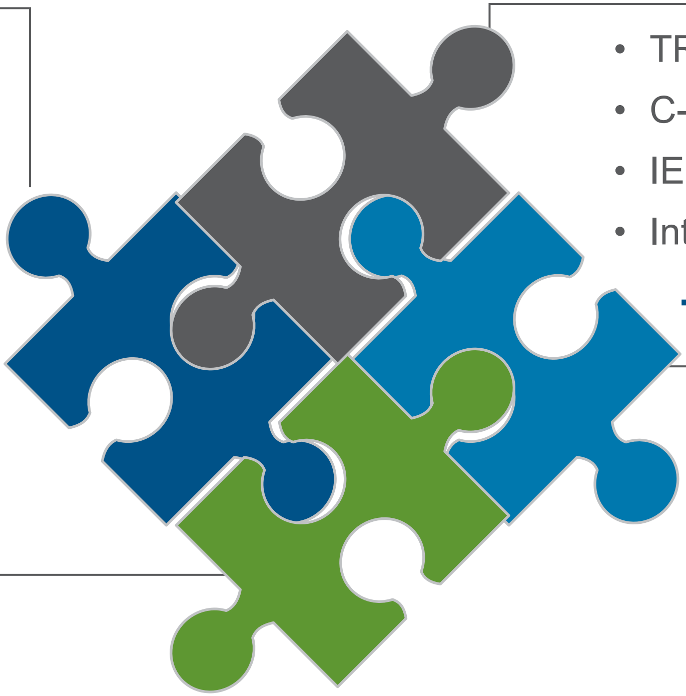
The CISA OBP leads the Department of Homeland Security's (DHS) efforts to implement National C-IED policy and enhance the Nation's ability to prevent, protect against, respond to, and mitigate the use of explosives against critical infrastructure; the private sector; and federal, state, local, tribal, and territorial entities.

Training & Awareness

- In-person Instructor-Led Training -In resident and Mobile Training Team
- Online Distance Learning - Virtual Instructor-Led trainings and web-based Independent Studies
- Learning Solutions Curriculum and Awareness Product Design and Development
- Train-the-Trainer Program

Policy Coordination

- Policy Design and Coordination
- Communications and Outreach
- C-IED Guidance and Product Design



Information Sharing

- TRIP*wire*
- C-IED and IED Information Sharing
- IED Incident and Threat Reporting
- Intra-agency Intelligence Coordination

Technical Assistance & Services

- C-IED Capability Assessments
- CI / Special Event Planning
- Explosive Blast Modeling
- C-IED Technology Development and Evaluation
- C-IED Grant Requirements Support

Counter-IED and Risk Mitigation Training

Develops and delivers a diverse curriculum of training and awareness products to build nationwide C-IED capabilities across the preparedness spectrum

Accredited training provider through the International Association for Continuing Education and Training (IACET) Meets American National Standards Institute (ANSI) requirements for excellence in instructional practices

Nationally Certified Program courses through IADLEST supporting law enforcement training academies and police and correctional officers

All training is provided free-of-charge

UNITED STATES DEPARTMENT OF HOMELAND SECURITY
CENTER FOR DOMESTIC PREPAREDNESS
FEMA

ACCREDITED IACET PROVIDER

CERTIFIED SAFETY ACT

DESIGNATED SAFETY ACT

DEVELOPMENTAL TESTING AND EVALUATION DESIGNATION SAFETY ACT

IADLEST Certified

IAEM International Association of Emergency Managers

C-IED Training Courses

OBP offers training to build C-IED capabilities through a variety of modalities to meet different stakeholders’ needs.

In-Person

- Bombing Prevention Awareness
- Bomb Threat Management Planning
- IED Search Procedures
- Protective Measures
- Surveillance Detection
- Vehicle-Borne Improvised Explosive Device Detection
- BMAP Community Liaison

Virtual Instructor

- IED Construction and Classification
- IED Explosive Effects Mitigation
- Introduction to the Terrorist Attack Cycle
- Homemade Explosives (HME) and Precursor Awareness
- Protective Measures Awareness
- Response to Suspicious Behaviors and Items
- Surveillance Detection Principles

Self-paced ISTs

- IED Awareness and Safety Procedures
- Homemade Explosives and Precursor Chemicals Awareness for Public Safety
- Bomb Threat Preparedness and Response
- Bomb-Making Materials Awareness: Your Role
- Bomb-Making Materials Awareness: Employee Training

Training Videos

- What to Do: Bomb Threat
- What to Do: Bomb Searches
- What to Do: Surviving a Bombing Attack
- What to Do: Suspicious or Unattended Item

Access courses at: cisa.gov/bombing-prevention-training-courses

Exercises

CISA conducts exercises with government, private sector, and international partners to enhance the security and resilience of critical infrastructure. Services include end-to-end exercise planning and conduct, CISA Tabletop Exercise Packages with over 80 scenarios, and national exercises.

Exercise Planning and Conduct

- Virtual
- In-person
- Discussion-based
- Operations-based

CISA Tabletop Exercise Package

- Civil disturbance
- Vehicle ramming
- Small UAS
- IED
- K-12 Education Active Threat
- Insider Threat
- Active Shooter
- And more

cisa.gov/critical-infrastructure-exercises

Cybersecurity Resources

- Cybersecurity Advisor Program
- Cybersecurity Assessments

Cybersecurity Advisor Program

- Cybersecurity Advisors (CSA) offer assistance to help prepare and protect private sector entities and governments from cybersecurity threats
  - **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 Services (Voluntary & No Cost)

Strategic

- Cyber Resilience Review (Strategic)
- External Dependencies Management (Strategic)
- Cyber Infrastructure Survey (Strategic)
- Cybersecurity Evaluation Tool (Strategic/Technical)

Tactical

- Phishing Campaign Assessment (EVERYONE)
- Vulnerability Scanning / Hygiene (Technical)
- Web Application Scanning (Technical)

STRATEGIC
(C-Suite Level)

TECHNICAL
(Network/System Admin Level)

Matthew Frost
Protective Security Advisor
South Florida
Matthew.frost@hq.dhs.gov