CISA

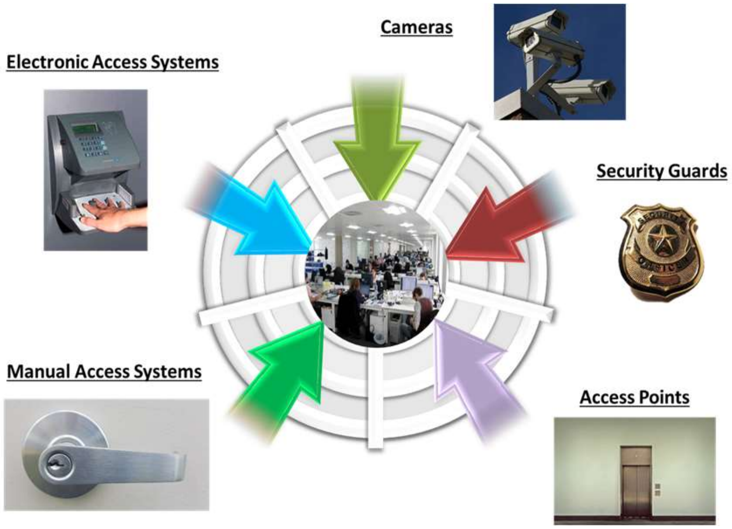
CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Protective Security Advisor Program

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



CISA Physical Security Assessments

- Security Assessment at First Entry (SAFE)
  - Quick look (2-3 hours) at the current security posture to identify vulnerabilities.
  - Written report of Commendables, Vulnerabilities, and Options for Considerations.
- Infrastructure Survey Tool
  - In-depth (4-6 hours) at physical security, protective measures, security force including dependencies.
  - Web-based survey tool and written report.

CISA Physical Security Resources

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.

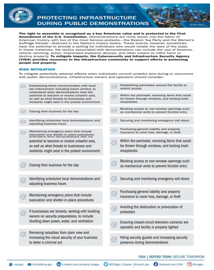
Vehicle Ramming Mitigation

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

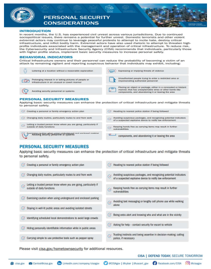
To mitigate potentially adverse effects when individuals commit unlawful acts during or concurrent with public demonstrations, infrastructure owners and operators should consider:

- ✓ 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 https://www.faa.gov/about/office_org/headquarters_offices/ash/ash_programs/investigations/leap/.

[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, https://www.faa.gov/uas/resources/community_engagement/no_drone_zone/.

[4] Refer to the full NOTAM here: https://www.faa.gov/uas/resources/policy_library/media/Sports_TFR_UAS_Handout.pdf and connect with federal, state, and local law enforcement to discuss enforcement options.

[5] To learn more about TFRs, visit https://www.faa.gov/pilots/safety/notams_tfr/.

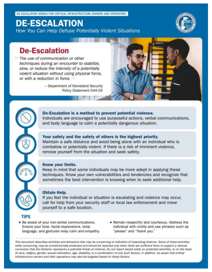
[6] For more information about FBI's potential criminal enforcement actions for violations of national defense airspace, refer to 14 CFR 99.7 and 49 U.S. Code § 46307.

[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

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 many more

cisa.gov/critical-infrastructure-exercises

Cybersecurity Advisor Program

Events in Alabama

- **Ransomware**
  - Social engineering- phishing and malware
    - Gootloader- asset management important
  - Ransome notifications via phone calls and voicemails
  - Compromised OT network resulting in IT network ransomware
- **Hactivists**
  - Cyber Av3ngers targeting Unitronics PLCs and default passwords
  - Pro-Russian targeting HMIs via VNC protocol over default port 5900
- **Volt Typhoon**
  - People’s Republic of China (PRC) state-sponsored cyber actors are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States.

Cybersecurity Services (Voluntary & No Cost)

- Vulnerability Scanning / Hygiene (CyHy)
- Web Application Scanning (WAS)
- Cybersecurity Performance Goals (CPG)
- Ransomware Readiness Assessment (RRA)
- Pen Testing
  - Remote Vulnerability Assessment (RVA)
  - Remote Penetration Testing (RPT)
- Validated Architecture Design Review (VADR)

Cybersecurity Services (Voluntary & No Cost)

- **Incident Management Review (IMR)**
- **Cyber Tabletop Exercises (CTTX)**
- **External Dependencies Management (EDM)**
- **Cyber Infrastructure Survey (CIS)**
- **Cyber Resilience Review (CRR)**
- **State and Local Cybersecurity Grant**
  - ALABAMA SLCGP PROGRAM

Report an Incident

- CISA: **cisa.gov/report** ; report@cisa.gov, (888) 282-0870
- FBI/ Internet Crime Complaint Center (IC3): **ic3.gov**

Cyber Threats of Today

Business Email Compromise

- 2 Billion in Loss
- Credential Stealing
- Phishing/ PopUps/ Poison Domains/ Onsite Exchange Vulnerabilities
- Steals Data
- Finance Diversions
- SupplyChain/External Dependencies Exploitation

Ransomware

- 700K per Victim
- Ransomware-As-A-Service Brokers – Gootloader
- Phishing-As-A-Service – Greatness (M365 exploitations)
- Lockbit, Blackcat, Royal, AlphV, Conti, Darkside
- Russian and North Korea State Actors
- Steals and Encrypts Data
- Double Extortion
- Destructive Malware Trends- Russia
    - Hermeticwiper and Wispergate

Denial of Service

- Russian-affiliated KILLNet Group
    - Feb 2023 Coordinated DDoS of Healthcare
- Dark Storm and Anonymous Sudan
    - Russian-Affiliated
    - Aug 2023 and March 2024 Threats to CI

Common Defensive Measures

- Multifactor Authentication (MFA)
- Backups- Off Network
- Vulnerability Management – Patching
- Configuration Management - RDP, SMB, etc
- Log Management and Review

Stephanie Watt
State Cyber Coordinator
Stephanie.Watt@cisa.dhs.gov
202-615-4615

Joe Parker
Cybersecurity Advisor North AL
Joseph.Parker@cisa.dhs.gov
202-894-4869

Clyde Roark
Cybersecurity Advisor South AL
Clyde.Roark@cisa.dhs.gov
850-776-2894

Kirk Toth
Protective Security Advisor South AL
Kirk.Toth@hq.dhs.gov
850-294-9300

Shirrell Roberts
Protective Security Advisor North AL
Aldolphus.Roberts@cisa.dhs.gov
202-923-0668

Derek Nesselrode
Emergency Communications Coordinator
Derek.Nesselrode@cisa.dhs.gov
202-731-3315