



PROTECTING INFRASTRUCTURE DURING PUBLIC DEMONSTRATIONS



DEFEND TODAY,
SECURE TOMORROW

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

RESOURCES

To support the infrastructure community in enhancing security, CISA provides access to a wide range of training, exercises, tools, and other materials focused on a variety of attack methods (active shooter, bombing, vehicle ramming, etc.), as well as other resources related to detecting behavioral indicators.

These resources provide valuable security and resilience information for the infrastructure community's consideration and offer entry points to many other CISA programs. For additional information regarding these resources contact central@cisa.gov.

Securing Soft Targets and Crowded Places (cisa.gov/securing-soft-targets-and-crowded-places)

Provides access to information regarding the types of threats posed to publicly accessible areas and resources with options for consideration to support risk mitigation activities.

CISA Bombing Prevention (cisa.gov/office-bombing-prevention-obp)

Maintains a range of actionable counter-improvised explosive device security and preparedness resources, including those focused on how to safely respond to bomb threats or suspicious items, gain threat and incident information, and access training and awareness videos to enhance preparedness.

Interagency Security Committee (cisa.gov/isc-policies-standards-best-practices)

Provides access to a series of best practices, standards, and guidance documents that are geared toward government facility security.

Protective Security Advisors (PSA) (cisa.gov/protective-security-advisors)

Provides access to a cadre of more than 100 subject matter experts located across the country who conduct infrastructure security and vulnerability mitigation activities at the local level.