IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

INTRODUCTION TO THE COMMERCIAL FACILITIES SECTOR RISK MANAGEMENT AGENCY

The Commercial Facilities Sector includes a diverse range of sites that draw large crowds of people for shopping, business, entertainment, or lodging. Facilities within this sector operate on the principle of open public access, meaning that the general public can congregate and move freely without highly visible security barriers. Most of these facilities are privately owned and operated, with minimal interaction with the federal government and other regulatory entities. As such, the day-to-day protection of commercial facilities is the responsibility of the owners and operators in close cooperation with local law enforcement. The potential for human and economic consequences underscores the need for the Federal Government and the Commercial Facilities Sector to work together to ensure the protection of these assets. The Cybersecurity and Infrastructure Security Agency (CISA) serves as the Sector Risk Management Agency (SRMA) for this sector. CISA works with private sector partners to defend against today's threats and collaboratively build more secure and resilient infrastructure for the future.

COMMERCIAL FACILITIES SECTOR COLLABORATION, RESOURCES, AND TRAINING

CISA offers many resources to help owners and operators manage risks, improve security, and aid the implementation and execution of protective and response measures across the Commercial Facilities Sector. This fact sheet lists a sampling of sector collaboration mechanisms, resources, and training materials. Unless otherwise noted below, additional information can be found on the CISA website at cisa.gov/commercial-facilities-sector.

Collaboration

Commercial Facilities Sector Government Coordinating Council (GCC), Sector Coordinating Council (SCC), and Working Groups convene regularly; share information; and develop tools, guidelines, and products. These groups work closely to plan, implement, and execute sector-wide resilience and security programs within the Commercial Facilities Sector.

The DHS Hometown Security initiative focuses on four steps—Connect, Plan, Train, Report—and provides tools and resources to help businesses improve proactive safety and security. Learn more at cisa.gov/hometown-security.

Protective Security Advisors are security subject matter experts who assist local efforts in protecting critical assets and provide a local perspective to the national risk landscape. Learn more at cisa.gov/protective-security-advisors.

The Homeland Security Information Network–Critical Infrastructure (HSIN-CI) Commercial Facilities Portal allows Commercial Facilities Sector partners to effectively collect and distribute security and resilience information for government and private sector partners.

Resources

Commercial Facilities Sector Cybersecurity Framework Implementation Guidance provides a common language that Commercial Facilities Sector owners and operators can use to assess and manage their cybersecurity risks and use the National Institute of Standards and Technology (NIST) voluntary Framework for Improving Critical Infrastructure Cybersecurity.

Commercial Facilities Sector Publications include the Protective Measures Guides, Public Venues Bag Search Procedures Guide, Public Venue Credentialing Guide, and other publications that help venues create and manage a safe environment for guests and employees. Learn more at cisa.gov/commercial-facilities-publications.

Business Continuity Planning Suite helps businesses create, improve, or update their business continuity plans with scalable, easy-to-use software. Learn more at ready.gov/business-continuity-planning-suite.

Training

Active shooter preparedness materials include a workshop series, online training, educational videos, and "How To Respond" resource materials, such as reference posters, guides, and cards. Learn more at cisa.gov/active-shooter-preparedness.

Self-paced, no-cost online training courses on active shooter preparedness, insider threat, surveillance detection, and more are available at training.fema.gov/is/cisr.aspx.

Webinars provide education and awareness for owners and operators on retail and hotel security, evolving threats to facilities, active shooter preparedness, and surveillance detection. Learn more at cisa.gov/commercial-facilities-training.

SECTOR PROFILE

Much of the Sector is privately owned and operated. It includes publicly traded companies and some publicly owned buildings (e.g., libraries, museums). Many facilities are considered soft targets—sites that are relatively vulnerable to a terrorist attack due to their open public access and limited security barriers. Commercial facilities are diverse in scope and function, ranging from small businesses to nationally and internationally recognized icons with large population densities when occupied. Owners and operators assess their specific facilities' vulnerabilities and provide the funding for risk mitigation measures, making cost a significant challenge to implementing security and resilience programs.

Sector Components

Media & Entertainment

Media production facilities, print media companies, and broadcast companies.

Gaming

Commercial and tribal casino operators, facilities, suppliers, and other entities affiliated with the gaming industry.

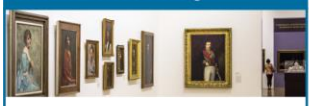
Lodging

Nongaming resorts, hotels and motels, hotel-based conference centers, and bed-and-breakfast establishments.

Outdoor Events

Amusement parks, fairs, exhibitions, parks, parades, marathons, and other outdoor venues and events.

Public Assembly



Convention centers, auditoriums, stadiums, arenas, and cultural properties like museums, zoos, and aquariums.

Real Estate

Office buildings and office parks, apartment buildings, multi-family towers and condominiums, self-storage facilities, and property management companies.

Retail

Malls, shopping centers, and strip malls, as well as freestanding retail establishments.

Sports Leagues

Major sports leagues and associations

CRITICAL INFRASTRUCTURE SECURITY CONSIDERATIONS

- **Armed Attacker:** Armed attacker events at shopping centers, office buildings, and open arenas are difficult to predict or prevent, particularly given the Sector's open access design. Combating this threat requires advanced planning, resources, and information sharing between commercial facilities subsectors and federal, state, and local security partners.
- **Cyberattacks:** The Commercial Facilities Sector widely uses the Internet for marketing, merchandising, ticketing, and reservations. A mass communications failure leading to a disruption of the Internet could affect the Sector as a whole and have cascading economic effects. Cyberattacks could also cause a loss of operations for automated building systems.
- **Supply Chain Disruptions:** Incredibly efficient supply chains have resulted in a "just-in-time" delivery model that leaves companies with minimal inventories, making some firms highly sensitive to supply disruptions. Supply chain disruptions could be the result of various causes, including geopolitical unrest, natural disasters, or tainted or counterfeit products.
- **Explosive Devices:** Attackers have used homemade explosives, or improvised explosive devices (IEDs), to attack commercial facilities to cause mass casualties and property damage. Open public access makes many facilities particularly vulnerable to explosives.
- **Unmanned Aircraft Systems (UAS):** Malicious actors could use UAS or drones to gain security knowledge or private information about a facility or event to carry out attacks. Drones could also be used for intellectual property theft or armed with a deadly weapon to execute terrorist attacks from the air.
- **Natural Disasters and Extreme Weather:** Severe weather events can cause significant property and economic damage; threaten the safety of employees and guests; and restrict access to critical resources, such as power, water, transportation, and food supplies.
- **Public Health Threats:** The Commercial Facilities Sector relies on large crowds and is one of the first sectors to feel the economic effect of threats to public health (e.g., pandemics).
- **Vehicle Ramming:** Perpetrators could deliberately ram a vehicle into a building, crowd of people, or another vehicle. Commercial vehicles present an especially attractive mechanism for vehicle-ramming attacks because they can penetrate security barriers, inflict large-scale damage, and have access to structures and activity centers.

FOR MORE INFORMATION ON THE COMMERCIAL FACILITIES SECTOR

Contact the Commercial Facilities Sector Management Team at CommercialFacilitiesSector@cisa.dhs.gov or learn more at cisa.gov/commercial-facilities-sector. For additional information about Commercial Facilities Sector, view the Commercial Facilities Sector-Specific Plan at cisa.gov/publication/nipp-ssp-commercial-facilities-2015.