
Homeland Security

# Introduction to the Commercial Facilities Sector-Specific Agency

The Commercial Facilities (CF) 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. The majority 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 underscore the need for the Federal Government and the CF Sector to work together to ensure the protection of these assets. The U.S. Department of Homeland Security (DHS), which serves as the CF Sector-Specific Agency (SSA), and sector partners collaboratively develop guidance, resources, and training that support the security and resilience of our Nation's prominent business centers and gathering places.

## Commercial Facilities Sector Collaboration, Resources, and Training

DHS 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 CF Sector. This fact sheet lists a sampling of sector collaboration mechanisms, resources, and training materials. Unless otherwise noted, additional information can be found on the DHS website at www.dhs.gov/commercial-facilities-sector.

### Collaboration

**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 www.dhs.gov/hometown-security.

**Protective Security Advisors** are security subject matter experts who assist local efforts to protect critical assets and provide a local perspective to the national risk picture. Learn more at www.dhs.gov/protective-security-advisors.

**Critical Infrastructure Cyber Community (C³) Voluntary Program** aligns business enterprises with existing resources to support cybersecurity risk management. Learn more at www.dhs.gov/ccubedvp.

### Resources

**CF Sector Publications** include the Protective Measures Guides, Mass Evacuation Planning Guide, Patron Screening Best Practices Guide, and more that help venues create and manage a safe environment for guests and employees. Learn more at www.dhs.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 www.ready.gov/business-continuity-planning-suite.

**Suspicious activity** videos and tools help owners, operators, and employees identify and report suspicious behavior and activity. Learn more at www.dhs.gov/commercial-facilities-resources.

### Training

**Active shooter preparedness** materials include a workshop series, online training, awareness videos, and "How To Respond" resource materials such as reference posters, guides, and cards. Learn more at www.dhs.gov/activeshooter.

Self-paced, no-cost **online training courses** on active shooter preparedness, insider threat, surveillance detection, and more are available at www.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 www.dhs.gov/commercial-facilities-training.

## Sector Profile

The majority of the sector is privately owned and operated, but 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 the vulnerabilities of their specific facilities and provide the funding for risk mitigation measures, making cost a significant challenge to implementing security and resilience programs.

## Trends and Emerging Issues

- **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, such as training material; and information sharing between CF subsectors and Federal, State, and local security partners.
- **Cyberattacks:** The 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 CF Sector as a whole and have cascading economic effects. Cyberattacks could also cause a loss of operations for automated building systems, giving hackers access to automated building systems and internal surveillance.
- **Supply Chain Disruptions:** Incredibly efficient supply chains have resulted in a "just-in-time" delivery model that leaves companies with very limited inventories, making some firms highly sensitive to supply disruptions. Supply chain disruptions could result from a range of 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 with the aim of causing 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 in order to carry out attacks. Drones could also be used for intellectual property theft, or could be 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 safety of employees and guests, and restrict access to critical resources such as power, water, transportation, and food supplies.

Commercial Facilities Subsectors

**Entertainment & Media**

49,024 establishments TV and movie production facilities, print media companies, and TV and radio broadcast stations

$1.4 trillion in total media spending annually

**Gaming**

1,392 casinos and associated resorts

Visited by 34% of U.S. adults in 2012

$38 billion in tax revenue


**Lodging**

52,887 hotel-based properties

$163 billion in annual sales

**Outdoor Events**

Fairs, exhibitions, outdoor venues, parades, and 564 amusement and theme parks

290 million visitors to amusement and theme parks in 2010

**Public Assembly**

124,773 establishments stadiums, arenas, movie theaters, and cultural properties such as museums, zoos, libraries, and performance venues

**Real Estate**

Includes 1 million office buildings, 5.6 million multi-family rental buildings, and over 48K self-storage facilities

Office buildings alone contribute $205.1 billion to U.S. GDP each year

**Retail**

1.1 million buildings malls, shopping centers, and retail

$2.5 trillion to U.S. GDP annually

**Sports Leagues**

134 million attendees at games last season (top-four major sports leagues)

The U.S. sports industry has an estimated size of $485 billion

Source: *2015 Commercial Facilities Sector-Specific Plan*

## For More Information on the Commercial Facilities Sector

- Contact the Commercial Facilities Sector-Specific Agency at cfsteam@hq.dhs.gov or learn more at www.dhs.gov/commercial-facilities-sector
- Commercial Facilities Sector-Specific Plan 2015: www.dhs.gov/publication/nipp-ssp-commercial-facilities-2015
- National Infrastructure Protection Plan (NIPP) 2013: www.dhs.gov/national-infrastructure-protection-plan
- Presidential Policy Directive 21, Critical Infrastructure Security and Resilience: www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil