# Commercial Facilities Sector-Specific Plan

## An Annex to the NIPP 2013

2015

Homeland Security

# TABLE OF CONTENTS

# COORDINATION LETTER FROM COUNCIL CHAIRS

In 2003, the Federal Government established the Commercial Facilities (CF) Sector as a critical infrastructure sector in the United States, recognizing that its security and resilience is essential to the economy and to public health and safety. Since that time, the sector has built strong partnerships that bring together private sector partners with their industry peers, as well as with government representatives at the Federal, State, and local levels. Together, those partners have improved information sharing, supported risk assessments, developed extensive guidance, and conducted training and exercises to improve security and resilience. The CF Sector keenly recognizes the value of this partnership and continues to take an active role in coordinated activities to improve the security and resilience of CF operations.

## 2015 Sector-Specific Plan Update

This 2015 release of the *Commercial Facilities Sector-Specific Plan* (SSP) updates the original plan issued in 2007 and the update issued in 2010. As with the previous plans, this SSP represents a collaborative effort among the private sector; Federal, State, local, tribal, and territorial governments; and nongovernmental organizations to reduce critical infrastructure risk.

The CF Sector Coordinating Council (SCC) and Government Coordinating Council (GCC) jointly developed the goals, priorities, and activities included in this SSP to reflect the overall strategic direction for the CF Sector. The Sector's goals support the Joint National Priorities developed in 2014 by the national council structures described in the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience (NIPP 2013)*.

This SSP also illustrates the continued maturation of the CF Sector partnership and the progress made to address the sector's evolving risk, operating, and policy environments.

## Key Accomplishments

Since 2010, CF Sector partners in the public and private sectors have taken significant steps to reduce sector risk, improve coordination, and strengthen security and resilience capabilities:

- Delivered a suite of active shooter programs and resources, including the delivery of over 100 active shooter preparedness workshops around the country, and the Active Shooter: What You Can Do (IS-907) course through the Federal Emergency Management Agency (FEMA) Emergency Management Institute.
- Assisted with the development and coordination of 78 security briefings and facilitated discussions across 33 States and Puerto Rico with the U.S. Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), private sector owners and operators, and local first responders to discuss operational responses and communication planning as a result of the Nairobi, Kenya, shopping mall attack.
- Participated in the *2012 National Infrastructure Advisory Council (NIAC) Intelligence Information Sharing* report that analyzed intelligence information sharing between DHS and private sector partners. The report examined whether or not the right people received the right intelligence information at the right time to support robust protection and resilience of the Nation's critical infrastructure, and provided recommendations to improve bidirectional information sharing.
- Worked with the Office of Intelligence & Analysis (I&A) to facilitate the Classified Intelligence Forum with the private sector. This provides appropriately cleared, identified members of the Critical Infrastructure Partnership Advisory Council (CIPAC) with access to classified draft or finished intelligence products to solicit feedback and gain overall customer insights.
- Developed the *Protective Measures Guides* for the U.S. lodging industry, commercial real estate, mountain resorts, and outdoor venues.
- Coordinated numerous Enhanced Security Outreach briefings around the country with DHS, General Services Administration (GSA), National Counterterrorism Center, and more following calls in extremist literature to target Federal and military installations.

- Developed no-cost, online training available through FEMA's Independent Study Program for active shooter preparedness, insider threat, surveillance awareness, and more.
- Delivered Airspace Security Summits around the country to examine the issue of Unmanned Aircraft Systems/ Remote Controlled Model Aircraft at commercial facilities.
- Established the Cyber Working Group to enhance cyber engagement throughout the sector.
- Added approximately 400 new documents to the CF portal on the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) and increased portal members by more than 50 percent from 2012 to 2013. Improved the CF portal by adding a feature that allows users to search by topic, improving the library's search and filtering tools, enhancing navigation, and highlighting content—such as incidents—that will improve users' situational awareness.
- Expanded efforts to assist public facilities with developing cyber and physical risk assessment plans, and shared risk reduction resources through direct consulting and speaking at industry meetings.
- Received Support Anti-terrorism by Fostering Effective Technologies Act (SAFETY Act) protections for facilities in the Sports Leagues, Real Estate, and Retail Subsectors. Established in 2002, the SAFETY Act created liability limitations for claims resulting from an act of terrorism where Qualified Anti-Terrorism Technologies have been deployed. For a full listing of Qualified Anti-Terrorism Technologies please visit www.safetyact.gov.
- Refined structure of the Retail Subsector by creating two councils within the subsector: the Shopping Center Subsector Council, which includes mall developers, and the Council of Retailers, which includes stores within malls and standalone retail establishments. This allows members to share information and to plan for events more efficiently.
- Expanded the Real Estate Information Sharing and Analysis Center (RE-ISAC) to include four of the eight subsectors—Gaming, Lodging, Real Estate, and Retail—and gained support from 10 associations.
- Collaborated with the FBI, Food and Drug Administration (FDA), and U.S. Department of Agriculture (USDA) Food Safety and Inspection Service to conduct pilot workshops for the Commercial Facilities Food Defense Initiative. This initiative assists commercial facilities that host large-scale events in mitigating vulnerabilities to an intentional food contamination incident involving the use of chemical, biological, or radiological (CBR) agents, and enhances coordination of response and investigative procedures.

These achievements, which represent a portion of the effective collaboration of the CF SCC, GCC, and Sector-Specific Agency (SSA), clearly demonstrate the sector's progress in working toward a rational approach to develop, prioritize, and implement effective security programs and resilience strategies.

In the same shared purpose that guided these actions and their support for the framework, concepts, and processes outlined in the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013) and Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity, CF Sector partners look forward to continuing their efforts to enhance the security and resilience of our Nation's critical infrastructure assets.

**Joseph B. Donovan**
Co-Chair
Commercial Facilities Sector
Coordinating Council

**Patrick Murphy**
Co-Chair
Commercial Facilities Sector
Coordinating Council

**Caitlin A. Durkovich**
Assistant Secretary
Office of Infrastructure Protection
U.S. Department of Homeland Security
Chair, Commercial Facilities Sector
Government Coordinating Council

# EXECUTIVE SUMMARY

The Commercial Facilities (CF) Sector is made up of an extremely diverse range of sites and assets where large numbers of people congregate daily to conduct business, purchase retail products, and enjoy recreational events and accommodations. Given the national and international visibility and potential human and economic consequences associated with commercial facilities, it is important for the Federal Government and the CF Sector to work together to ensure the protection of our Nation's prominent business centers and gathering places.

## Commercial Facilities Sector Assets and Risks

The majority of CF Sector facilities are privately owned, operate with minimal regulations, and house the business activities and commercial transactions that dominate the U.S. economy. The sector is divided into eight subsectors—Entertainment and Media, Gaming, Lodging, Outdoor Events, Public Assembly, Real Estate, Retail, and Sports Leagues—to facilitate coordination among facilities with similar functions, operations, and security issues. The Retail Subsector is further divided into two councils: the Shopping Center Subsector Council, which includes mall developers, and the Council of Retailers, which includes stores within malls and standalone retail establishments. While diverse, CF stakeholders, facing common existing and developing risks, must balance security priorities with their need for open access, public confidence, and economic vitality.

Natural disasters, armed attacker and terrorist threats, pandemics, theft, supply chain, and geopolitical disruptions are persistent risks to the CF Sector. Risks associated with cyberattacks continue to grow, as CF Sector reliance on cyber systems, such as for online financial transactions and building management, rises. The use of social media has facilitated increasingly coordinated protest activities and has also allowed terrorist organizations to solicit support. The CF Sector is also working on collaborating with the Federal Aviation Administration (FAA) to address risks posed by the growing prevalence of unmanned aircraft systems (UAS) or drones.

## Partnering to Improve Security and Resilience

When owners and operators better understand their risks and interdependencies, they can develop business continuity strategies that build agility and redundancy into operations and implement security practices that mitigate facility and asset risks. Each company is responsible for managing individual operational risks. Owners and operators in the CF Sector assess individual risks and establish internal plans to mitigate risks and respond to disruptions.

The *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013) partnership structure enables owners and operators to work directly with their peers through the Sector Coordinating Council (SCC) and with Federal, regional, and local partners through the Government Coordinating Council (GCC). Partners collaborate on a voluntary basis to share actionable, relevant risk information; exchange best practices; build cross-sector situational awareness; and enable risk-informed decision-making.

Through this partnership, the CF Sector has developed tools, resources, and programs that support sector-wide risk management and maximize partners' resources. Key examples include conducting vulnerability assessments of high-priority infrastructure; developing Webinars, threat briefings, tabletop exercises, and training; and collaborating with State, local, and regional authorities to build disaster response.

## 2015 Sector-Specific Plan

This *Commercial Facilities Sector-Specific Plan* (SSP) is designed to guide the sector's voluntary, collaborative efforts to improve security and resilience during the next four years. It describes how the CF Sector manages risks and contributes to national critical infrastructure security and resilience, as set forth in Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience. As an annex to the NIPP 2013, this SSP tailors the strategic guidance provided in the NIPP 2013 to the unique operating conditions and risk landscape of the CF Sector. As such, the sector strategy supports the NIPP 2013 national goals and strategy, the 2014 Joint National Priorities, and implementation of Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity.

The CF Sector aligned its SSP with the national planning framework for security and resilience in the NIPP 2013. As a result, progress toward sector goals, priorities, and activities contributes directly to national achievements under the NIPP 2013. Appendix B demonstrates the detailed alignment of this SSP to NIPP 2013 goals, the Joint National Priorities, and the NIPP 2013 Calls to Action.

## Sector Goals, Priorities, and Activities

As part of this 2015 SSP, the CF SCC and GCC have identified goals and priorities to guide the sector's security and resilience efforts over the next four years and to meet the sector's risk profile. As part of a detailed implementation plan, the sector identified 24 activities that partners plan to undertake, as resources allow, to improve the security and resilience of U.S. CF operations.

Table ES-1. 2015 Commercial Facilities Sector Goals and Priorities

| Goals | Priorities | |
|---|---|---|
| 1 Strengthen trusted and protected information sharing and ensure sector access to timely, actionable, and threat-specific information and analysis. | PRIORITY A | Improve formal public-private information-sharing processes at all levels; expand owner and operator access to relevant intelligence; and centralize two-way, public-private threat sharing to streamline reporting. |
| | PRIORITY B | Promote value of participation in the sector partnership to better engage and reach out to all subsectors, smaller owners and operators, and industry organizations in the sector partnership. |
| 2 Support the sector's needs for open access, public confidence, and economic vitality while cost-effectively reducing physical and cyber risks and enhancing overall security and resilience. | PRIORITY C | Expand upon sector products, training, and exercises to enable owners and operators to reduce risk and improve readiness. |
| | PRIORITY D | Improve CF cybersecurity knowledge, tools, capabilities, risk assessments, and practices to secure critical cyber and physical assets linked to cyber systems. |
| 3 Increase capabilities and maintain advanced planning systems to ensure timely and effective response and recovery of critical services. | PRIORITY E | Enhance coordination with interdependent sectors and community response partners to improve resilience and enhance decision-making. |
| 4 Assess and analyze threats, vulnerabilities, and consequences to inform facility and sector-wide risk management. | PRIORITY F | Continue to conduct cyber and physical risk assessments and develop risk reduction strategies for evolving threats in collaboration with cross-sector, Federal, regional, and local security stakeholders. |
| 5 Promote continuous learning and adaptation during exercises, incidents, and planning. | PRIORITY G | Share security and resilience best practices and case studies to enable owners and operators to leverage lessons learned in all risk mitigation activities. |

Table ES-2. 2015 Commercial Facilities Sector Activities Mapped to Priorities

| Map to Priority | | Sector Activities |
|---|---|---|
| A B | 1 | Improve DHS coordination with other Federal, State, regional, and local agencies—including the Federal Protective Service and General Services Administration—and centralize government sources for CF owners and operators to access information from across all agencies, including fusion centers. |
| A B | 2 | Formalize the process across DHS to provide sector feedback on intelligence that should be delivered at the For Official Use Only level. Increase the number of clearances in each CF subsector. |
| A B | 3 | Promote coordination among 77 fusion centers to connect nationwide information, particularly for national and global corporations. Use the Real Estate Information Sharing and Analysis Center as a resource. |
| A B | 4 | Increase awareness of the sector partnership framework, available resources, and strategic value to better engage all subsectors and small-scale owners and operators and to recruit new members. Engage unions, Chambers of Commerce, and the Small Business Administration in security awareness training activities. |
| A B | 5 | Continue to expand the Real Estate Information Sharing and Analysis Center to include the Entertainment and Media, Outdoor Events, Public Assembly, and Sports Leagues Subsectors, and strengthen information-sharing relationships with owners and operators. |
| B | 6 | Reevaluate and restructure the CF Sector to optimize organization and reflect relationships between subsectors. |
| A F | 7 | Continue to conduct outreach for existing risks assessment tools/resources and leverage them to conduct onsite risk assessments at high-priority facilities. |
| C D | 8 | Leverage cyber-assessment capabilities from DHS and other Federal agencies to conduct onsite assessments and share common vulnerabilities across subsector facilities. |
| D | 9 | Evaluate potential cyber risks and encourage CF Sector members to use the National Institute for Standards and Technology Cybersecurity Framework. Formulate communities of subsector information technology experts (connected to the Sector Coordinating Council) to address sector-specific cyber threats. |
| B C | 10 | Expand armed attacker training to help smaller companies prepare and to provide materials for owners and operators to address employee training gaps. |
| B C G | 11 | Develop surveillance curriculum for security directors and leaders within the Surveillance Awareness Working Group. |
| B C E G | 12 | Develop a Sector Coordinating Council playbook for government and industry coordination and communication protocols during disaster response and recovery. |
| C E F | 13 | Develop an inventory of all documents and guides in each subsector. |
| A C F G | 14 | Track after-action reports from previous events across critical sectors to completion. |
| C E F | 15 | Work with the lifeline sectors, particularly the Energy and Water sectors, to examine strategies to sustain CF Sector operations during an interruption of services, such as by holding joint exercises, creating cross-sector councils, identifying ideas to improve resiliency, or organizing other activities. |
| E F | 16 | Work with the Emergency Services Sector and local officials to develop and conduct outreach for low-cost, unified, and nationwide response efforts—such as crisis reentry credentialing to ensure access to restricted areas after a disaster. |
| B F | 17 | Facilitate collaboration among owners, management companies, and tenants—along with Federal, State, and local partners—to improve joint risk mitigation and response to armed attacker threats. |
| E F | 18 | Collaborate with the Financial Services Sector to create a joint resource for logging the accessibility of ATM and banking resources during disasters, leveraging the Financial Services Information Sharing and Analysis Center and the Real Estate Information Sharing and Analysis Center. |

| Map to Priority | | Sector Activities |
|---|---|---|
| B G | 19 | Work with Outdoor Events Subsector partners to increase resilience of outdoor events. |
| F G | 20 | Identify regions most at risk from climate change, determine which factors place them at risk, and develop mitigation strategies for CF infrastructure. |
| F G | 21 | Work with government and private sector partners, including the Federal Aviation Administration, to evaluate the emerging risk of unmanned aircraft systems and develop response strategies. |
| F G | 22 | Improve the sector's ability to leverage and respond to social media to enhance security during incidents and steady-state operations. |
| B G | 23 | Encourage more CF partners to seek SAFETY Act designation or certification, where appropriate. |
| A C E | 24 | Build on the Resilience Measurement Index to establish a resilience "score card" that helps owners and operators in the CF Sector and lifeline sectors determine how resilience is being measured and managed, and assists government agencies with tracking their effectiveness in information sharing. |

# 1 INTRODUCTION

This *Commercial Facilities Sector-Specific Plan* (SSP) sets the strategic direction for voluntary, collaborative efforts to improve sector security and resilience over the next four years. It describes how the Commercial Facilities (CF) Sector manages risks and contributes to national critical infrastructure security and resilience, as set forth in Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience. As an annex to the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience (NIPP 2013)*, this SSP tailors the strategic guidance provided in the NIPP 2013 to the unique operating conditions and risk landscape of the CF Sector. As such, the sector strategy supports the NIPP 2013 national goals and strategy, the 2014 Joint National Priorities, and implementation of Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity.

This plan describes the CF Sector's approach to risk management and national preparedness—considering its distinct assets, operations, and risk profile. Public and private sector members of the CF Sector Coordinating Council (SCC) and Government Coordinating Council (GCC) identified a shared vision, goals, and priorities for sector security and resilience. They developed a supporting set of collaborative activities they plan to pursue during the next four years, as resources allow.

SSP development answers NIPP 2013 Call to Action #2, which requires each of the 16 designated critical infrastructure sectors to update their SSP every four years to reflect joint priorities, address sector reliance on lifeline functions, describe national preparedness efforts, outline cybersecurity efforts, and develop metrics to measure progress. Appendix B illustrates how the CF Sector's goals, priorities, and activities support the 5 NIPP 2013 national goals, the 5 Joint National Priorities, and the 12 NIPP 2013 Calls to Action.

The remainder of this CF SSP includes:

- **Chapter 2: Sector Overview**—Provides a view of the sector's assets and operating characteristics, risk profile, and key public and private sector partners.
- **Chapter 3: Risk Management and National Preparedness**—Describes the mechanisms to achieve sector goals, including ongoing and planned partnership programs, activities, and resources that support the sector's current risk management approach; research and development (R&D) priorities; and how the sector supports national preparedness through incident response and recovery.
- **Chapter 4: Vision, Goals, and Priorities**—Presents the sector's vision, updated goals and priorities for CF security and resilience for the next four years, and the specific activities CF Sector public and private sector stakeholders plan to conduct.
- **Chapter 5: Measuring Effectiveness**—Describes the planned approach the sector will use to measure the effectiveness of individual activities.

This SSP provides targets for collaborative planning among the U.S. Department of Homeland Security (DHS), as the Sector-Specific Agency (SSA), and CF SCC and GCC members. Partners have a clear and shared interest in ensuring the security and resilience of critical sector assets, systems, and networks, and this plan represents the voluntary, collaborative activities that could greatly reduce sector risk and build resilience during the next four years.

# 2 SECTOR OVERVIEW

This chapter profiles the Commercial Facilities (CF) Sector's assets, design, and operating characteristics; identifies its primary risks and interdependencies; and describes how the sector's public-private partnership operates.

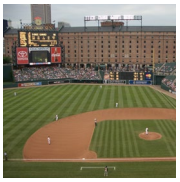
## 2.1 Sector Profile

The CF Sector is made up of an extremely diverse range of sites and assets where large numbers of people congregate daily to conduct business, purchase retail products, and enjoy recreational events and accommodations. The majority of facilities have open public access and house the business activities and commercial transactions that dominate the U.S. economy. CF stakeholders must balance security priorities with their need for open access, public confidence, and economic vitality. In general, commercial facilities are privately owned and operated with minimal oversight from Federal, State, and regional government regulatory entities; however, government facilities may reside within commercial properties. Assets can range from as small as a one-room museum to stadiums that can host events large and high-profile enough to be designated as National Special Security Events (NSSEs) by the Secretary of Homeland Security. The following overview provides a snapshot of CF Sector assets and operations.

### Key Sector Operating Characteristics

Facilities and events primarily operate on the principle of **open public access**, meaning people may move freely through the facilities without the deterrent of highly visible security barriers. This layout can go against design security principles. Additionally, high-profile tenants, neighbors, and special events may add risks to individual assets.

Many facilities are considered **soft targets**—sites that are relatively vulnerable to a terrorist attack due to their open access and **limited security barriers**. This makes intelligence and information sharing especially critical in recognizing and monitoring trends and thwarting attacks.



Many facilities, such as stadiums, malls, and museums, are **nationally and internationally recognized icons** and have **large population densities** when occupied, which increases their likelihood of being targeted by adversaries. Facility attendance can act as a barometer of public confidence in national security.

High economic significance and public safety implications result in a **large national security interest** in facilities that are privately owned and secured. This dynamic necessitates a strong information-sharing relationship between owners and operators and their Federal, State, and regional government intelligence partners.

Although commercial facilities are **widely dispersed**, certain subsectors are concentrated in specific regions, necessitating regional security coordination between private and government partners. The Entertainment and Media Subsector, for example, has hubs in Los Angeles and New York City, while the two biggest markets for the Gaming Subsector are in Las Vegas and Reno, NV, and Atlantic City, NJ.

Given CF Sector's significant **impact on the economy**, reestablishing the sector's assets after a disaster is required to secure local and State financial security.

# COMMERCIAL FACILITIES SECTOR SNAPSHOT

## ASSETS AND IMPACTS

### Entertainment & Media

**49,024 establishments** TV and movie production facilities, print media companies, and TV and radio broadcast stations[1]

**$1.4 trillion** in total media spending annually[2]

### Gaming[3]

**1,392 casinos and associated resorts**

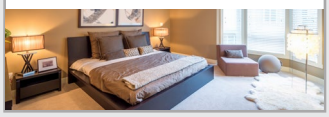
Visited by **34% of U.S. adults** in 2012

**$38 billion** in tax revenue


### Lodging[4]

**52,887 hotel-based properties**

**$163 billion** in annual sales



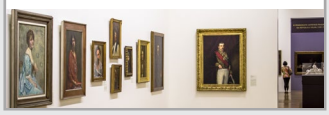
### Outdoor Events

Fairs, exhibitions, outdoor venues, parades, and **564 amusement and theme parks**[5]

**290 million visitors** to amusement and theme parks in 2010[6]

### Public Assembly[7]

**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**[8], **5.6 million multi-family rental buildings**[9], and over **48K self-storage facilities**[10]

Office buildings alone contribute **$205.1 billion** to U.S. GDP each year[11]

### Retail

**1.1 million buildings** malls, shopping centers, and retail[12]

**$2.5 trillion** to U.S. GDP annually[13]

### Sports Leagues

**134 million attendees** at games last season (top-four major sports leagues)[14]

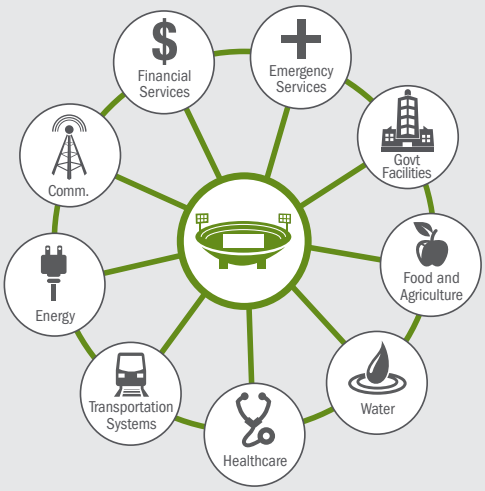
The U.S. sports industry has an estimated size of **$485 billion**[15]

## OWNERS AND OPERATORS

- The majority of the sector is **privately owned and operated**, but includes publicly traded companies and some publicly owned buildings (e.g., libraries, museums).
- **Owners and operators** assess vulnerabilities of their specific facilities and practice prudent risk management and mitigation measures.
- Individual owners and operators most commonly provide funding for security and resilience programs, making **cost a significant challenge** to implementing modern security programs.

## CRITICAL SECTOR INTERDEPENDENCIES

Without energy, communications, and potable water, the CF Sector would not be able to sustain operations. Transportation systems allow employees and customers to travel to and from facilities and enable facilities to receive products and supplies. The CF Sector partners regularly with Emergency Services personnel to mitigate risk, and the Emergency Services Sector responds to disasters that occur at facilities. Healthcare partners provide services to the public after an event, including a large-scale outbreak of an illness. The CF Sector relies on financial services to conduct daily business operations, and the Financial Services Sector needs the CF Sector for its facilities. Government facilities sometimes reside within CF Sector properties as tenants or adjacent to commercial facilities. This affects the risk of the CF and Government Facilities Sectors, which collaborate to address security challenges, and could impact continuity of government operations and timely recovery from events. The CF Sector depends on the Food and Agriculture Sector for food and beverages served at commercial facilities.



# Sector Components and Assets

The CF Sector represents a huge number of facilities and sites that are diverse in size, function, operating principles, and security risks. The sector is divided into eight subsectors—Entertainment and Media, Gaming, Lodging, Outdoor Events, Public Assembly, Real Estate, Retail, and Sports Leagues—to facilitate coordination among facilities with similar functions, operations, and security issues. The Retail Subsector is further divided into two councils: the Shopping Center Subsector Council, which includes mall developers, and the Council of Retailers, which includes stores within malls and standalone retail establishments. The following sections provide brief overviews of the assets and key security and resilience considerations unique to each subsector.

Despite their differences, nearly all commercial facilities are privately owned and operated with minimal regulations. Structures and establishments in every subsector are almost entirely regulated at the State and local levels through building codes and requirements geared toward improving the safety of employees and visitors. Federal oversight is mostly limited to safety- or access-related requirements of the Occupational Safety and Health Administration (OSHA) and Americans with Disabilities Act (ADA), or standards from the National Fire Protection Association (NFPA).

These codes and regulations are not focused on resilience. As a result, individual owners and operators take responsibility for assessing facility risks and implementing risk management and mitigation actions. Owners and operators within each subsector have formed associations, working groups, the Real Estate Information Sharing and Analysis Center (RE-ISAC), and other mechanisms to facilitate intelligence and risk information sharing and to exchange best practices and tools for security and resilience.

## Entertainment and Media Subsector

**Print Media**
40M paid daily subscribers

**Media Production**
1.9M workers and 659 films in the U.S. in 2013

**Broadcast**
30,460 stations contribute up to 7% of U.S. GDP

The subsector includes media production facilities (e.g., television and motion pictures), print media companies (e.g., newspapers, magazines, and books), and broadcast companies (e.g., television and radio stations). These outlets reach the general population on a continuous basis and have a significant effect on the economy. Newspapers boast 40 million paid daily subscribers,[16] while 30,460 television and radio broadcast stations[17] contribute up to 7 percent of the U.S. gross domestic product (GDP),[18] and the movie industry supports 1.9 million workers and released 659 films nationwide in 2013.[19]

### Key Asset Considerations

#### Relatively Limited Access

Unlike the majority of the CF Sector, Entertainment and Media Subsector facilities are generally closed to the public and employ visible security barriers and access control measures.

#### High-Profile Celebrities and Media Outlets

High-profile celebrities are regularly present on studio sites, requiring security procedures to deal with the public, paparazzi, and stalkers. Stars often have private security details as well. Recently, the paparazzi have started to use drones to capture pictures in studio areas. News and broadcasting facilities may also attract the attention of attackers due to having a high public profile. This may particularly affect facilities in large metro areas where the public can park and congregate near broadcast buildings.

#### Geographical Concentration

Major movie studios are located in relatively close proximity in the Los Angeles area and often have corporate affiliations with television studios in the New York City area.

#### Self-Contained Services

Primarily on the West Coast, larger movie studios operate like small cities and maintain their own emergency services equipment and personnel. The studios also coordinate closely with each other, county and city police, and fire departments. In some cases, studio employees receive search and rescue, earthquake response, and emergency medical service training.

#### Hacking and Piracy

Hacking and piracy are major concerns for studios. The distribution of a film prior to its release or the release of business

documents and correspondence could cost a studio millions of dollars. Employees use electronic access cards to enter studio sites and are subject to many of the same security measures as visitors (e.g., bag searches).

## Gaming Subsector

**Employment**
The subsector supports over 1.7M jobs

**Economic Output**
$240B contributed to U.S. economy


**Tax Revenue**
$38B in local, State, and Federal tax revenue

The subsector includes commercial and tribal casino operators, cyber and physical assets, suppliers, and other entities affiliated with the gaming industry. Assets are located in 40 States across the country. The gaming industry contributes $240 billion to the U.S. economy and supports more than 1.7 million jobs and nearly $74 billion in income. It also generates $38 billion in tax revenues to local, State, and Federal governments.[20] Tribal governments operate 499 gaming facilities in 28 States[21] and generated $28 billion in gross gaming revenue in 2013.[22] The National Indian Gaming Commission is responsible for regulating gaming on Indian lands.

### Key Asset Considerations

#### Small Cities

A large gaming facility complex is like a small city, with numerous types of large facilities (e.g., casinos, convention centers, performance venues, hotels, restaurants, and shopping centers) under one roof. In major casino markets, gaming facilities are grouped close together in a "strip" area, creating several small cities in a relatively small geographical area. These gaming facilities employ large staffs and welcome large numbers of visitors.

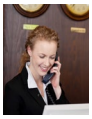
#### 24/7 Operations

The casino portion of a gaming facility complex operates under an open public access model, 24 hours a day, 7 days a week. Although there may be access control measures in other parts of the complex (e.g., tickets are required in a theater), casino customers enter and exit the facility continuously and freely.

#### Sophisticated Surveillance

Casino gaming complexes are typically a mix of open/unrestricted access (gaming and restaurant areas) and also highly restricted access areas (closed-circuit television, security command, information technology, and currency storage areas that contain large amounts of cash). Although access controls are not employed to gain entrance onto a casino floor, a sophisticated array of surveillance measures continuously monitors activities in that area. State gaming commissions regulate the gaming part of casino operations and can establish specific standards for security and surveillance (e.g., the number and type of cameras, pixels of resolution, the number of security guards in the gaming areas).

## Lodging Subsector



**Employment**
The subsector employs over 1.9M people

**Economic Output**
Travel and tourism generates $2.1T in economic activity

The subsector includes nongaming resorts, hotels and motels, hotel-based conference centers, and bed-and-breakfast establishments. Travel and tourism is the sixth-largest employer in the United States and generated $2.1 trillion in economic output in 2013.[23] Accommodations makes up the largest portion of this industry—contributing nearly one-fifth of its total output[24]—and supports 1.9 million hotel property workers.[25]

Hotels range from stand-alone, multistory structures located in the downtown business district of a city, to structures of only a few stories spread out over many acres in a resort setting. Hotels can be found in almost all of the other CF subsectors.

### Key Asset Considerations

#### Continuous Occupancy

Unlike many other commercial facilities, hotels and motels are occupied around the clock. People can eat, sleep, conduct business, and take part in entertainment activities within the same facility over multiple days.

### Emergency Shelters
Hotels and motels have been used as shelters during natural disasters. Owners and operators have performed services such as collaborating to find rooms for disaster victims and making properties available in times of need.

### Self-Contained
Some hotels operate similar to small cities. They are capable of generating their own electrical power and they operate their own water filtration and wastewater treatment facilities. Many full-service hotels have restaurants, shops, and meeting rooms. Convention centers, shopping malls, sports facilities, office buildings, and public transportation facilities may be adjacent to or integrated into the hotel facility.

### Just-In-Time Buyers
Many hotels are "just-in-time" buyers. They often rely on the Internet to place orders and on the transportation and commercial distribution systems to deliver goods and services when needed. This results in fresh food and supplies being available without the need to store, prepare, or process them onsite. However, this reliance on just-in-time supply chains creates the potential for a lack of sufficient supplies if the hotel is used for shelter during a disaster.

### High-Profile Guests and Events
High-profile hotel guests—such as dignitaries and celebrities—and events—such as a military ball or religiously affiliated conference—increase a hotel's security risks. This requires security procedures to ensure a facility's resilience. Clients and events may also provide private security details.

## Outdoor Events Subsector

**Attendance**
The Macy's Thanksgiving Day Parade draws more than 3.5M people

**Economic Output**
Amusement parks contribute about $57M to the economy

**Frequency**
Over 3,200 fairs are held in North America each year

The subsector includes amusement parks, fairs, exhibitions, parks, parades, marathons, and other outdoor venues and events. Over 3,200 fairs are held in North America each year,[26] including large State fairs with an attendance of more than a million people in a two- or three-week period. Amusement parks are more permanent, generate about $12 billion in revenues, and contribute about $57 million to the economy.[27] Parades in large cities can draw millions of spectators, such as the Macy's Thanksgiving Day Parade, which attracts more than 3.5 million people to the streets of New York City each year, and is watched on television by another 50 million people.[28]

The subsector represents those activities and gatherings of people that take place outdoors, although there are usually buildings (e.g., restaurants, snack bars, hotels, shops, barns, and exhibition halls) associated with the activity. The outdoor nature of the event may sometimes result in attendees being spread out over a larger area than they would have been if the event had taken place in an enclosed structure.

### Key Asset Considerations

#### Diversity
The Outdoor Events Subsector represents an exceptionally diverse range of facilities and activities, from large, established theme parks with annual attendance in the millions, to festivals and parades with attendance in the thousands over a period of hours.

#### Perimeter
Some events (e.g., parades, festivals, and carnivals) take place not only outside, but in an open environment with no established perimeter or access controls.

#### Seasonality
Many outdoor events are seasonal or last only a few weeks, days, or hours. Vendors and suppliers, as well as security personnel who service the event, are not permanent employees, but are hired for the length of the event. Some employees are foreign nationals, working through visas that allow for temporary, non-agricultural jobs. In addition, large numbers of volunteers may be involved in staffing the event.

#### Small Cities
Some of the larger theme parks may function like small cities, with restaurants, hotels, and other diverse facilities on the premises.

### Ownership

The assets are generally owned and operated by private sector companies or cooperatives, although local government may own or sponsor some venues, such as public parks or fair grounds.

## Public Assembly Subsector

**Movie Theaters**
1.3B tickets sold per year

**Zoos & Aquariums**
$16B in economic output and 142,000 jobs

**Museums**
$21B contributed to the U.S. economy each year

The subsector includes assets where a large number of people congregate: convention centers, auditoriums, stadiums, arenas, movie theaters, and cultural properties (e.g., museums, zoos, planetariums, aquariums, libraries, and performance venues). Many facilities experience high levels of attendance. For instance, movie theaters sell 1.3 billion tickets each year.[29] The subsector also has a significant effect on the economy. Museums directly contribute $21 billion to the U.S. economy each year.[30] Accredited zoos and aquariums contribute $16 billion to the U.S. economy and support 142,000 jobs.[31]

### Key Asset Considerations

#### Diversity

The size, utilization, and owner-management formats of public assembly facilities vary greatly. For example, museums and libraries may be found in one room of a building or incorporate multiple buildings located throughout a city or State.

#### Emergency Shelters

Public assembly facilities provide extended shelter and comfort for displaced individuals during an incident. These facilities may also serve as emergency services command centers for local and Federal first responders.

#### Command Center

Many public assembly facilities with high attendance numbers use a command center to monitor activities. This can serve as an operations center in the event of a manmade or natural incident.

#### Ownership

Public assembly facilities that are privately owned and operated are more likely to utilize a private security company. However, some local jurisdictions require the use of their own law enforcement officers.

## Real Estate Subsector

**Economic Output**
Represents 13% of GDP by revenue

**Residential**
18M multifamily households

**Self-Storage**
48,500 self-storage facilities in the U.S.

The subsector includes office buildings and office parks, apartment buildings, multifamily towers and condominiums, self-storage facilities, and property management companies. These facilities comprise the properties many Americans live and work in every day. There are over 18 million multi-family households across the United States.[32] The commercial real estate market is vital to the economy, representing 13 percent of GDP by revenue and generating or supporting 9 million jobs.[33] A survey by the Building Owners and Managers Association tallied 9.9 billion square feet of office space among its members.[34] There are approximately 48,500 self-storage facilities in the United States and 4,000 facilities where self-storage is a secondary source of revenue.[35]

Traditionally, terrorists have selected buildings (primarily commercial buildings) as the preferred target of attacks. The collapse or failure of these buildings can have a severe effect on all sectors of the economy—including Federal, State, and local—and key resources, and can result in significant loss of life.

### Key Asset Considerations

#### Continuous Occupancy

The Real Estate Subsector experiences continuous occupation because the public both lives and works within this subsector's facilities.

### Division of Responsibility between Owners and Tenants

Tenants renting space in commercial real estate facilities, such as commercial office buildings and residential buildings, are typically responsible for their own safety in any scenario short of emergency evacuation, and each has their own corporate security and policies. The property manager of a facility is responsible for perimeter access controls and continuity of critical functions (e.g., water pumps, heating and air conditioning systems, evacuation planning), as well as lifeline services supplied by local utilities.

### Tenant/Resident Identification

Residential property owners and operators screen all rental applicants using credit reports, criminal background databases, and Federal terrorist watch lists prior to granting residency. This information is used to ensure the suitability of the renter, financial security for the owner, and the safety of existing and future building occupants. Some buildings house high-risk tenants (e.g., high-profile government tenants) and special-use tenants (e.g., banking facilities) or a mixture of both high- and low-risk tenants.

### Subcontracting

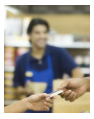
A vulnerability of the commercial real estate industry is the lack of security controls with regard to cleaning and groundskeeping services, including the issue of illegal subcontracting. Many janitors, for example, have nearly unlimited access to a building's sensitive areas during and after working hours. If this position were illegally subcontracted, it could allow terrorists, criminals, and former or disgruntled employees to infiltrate and exploit a building.

### Faith-based Facilities

Although religious facilities sometimes reside within commercial real estate facilities, the CF Sector is not the Sector-Specific Agency for these organizations. The Homeland Security Advisory Council established the Faith-based Communications and Security Advisory Committee to provide recommendations and explore current and potential security information-sharing opportunities and methods between the Department of Homeland Security (DHS) and faith-based organizations.

## Retail Subsector

**Employment**
25% of US jobs (42M positions)



**Economic Output**
One-fifth of the total U.S. economy

The subsector includes tenant space in enclosed malls, shopping centers, and strip malls, as well as freestanding retail establishments. The subsector is divided into two councils: the Shopping Center Subsector Council, which includes mall developers, and the Council of Retailers, which includes stores within malls and standalone retail establishments. The subsector is the Nation's largest private sector employer, accounting for one in four U.S. jobs, which totals about 42 million positions. The subsector also makes up one-fifth of the total U.S. economy.[36] Online shopping reached $262 billion in 2013, and could grow to $370 billion in 2017.[37]

### Key Asset Considerations

#### Multiple Access Points

Retail establishments have open access for the public, and do not require fees, tickets, or reservations. Establishments have more than one access point for customers, personal vehicles, and delivery trucks.

#### Frequency and Volume of People

Retail establishments are surrounded daily by a steady flow of traffic because they provide basic necessities to the population. In the case of enclosed malls that house independently-owned retail tenants, controlling who enters and exits is especially difficult. Patrons also generally carry bags and packages within shopping facilities, which could easily conceal various types of weapons.

#### Highly Competitive

Competition and economic conditions force owners and operators to minimize highly visible or obtrusive protective measures, because these can make prospective patrons uneasy. Retailers strive to maintain the highest reputation possible because customers can easily go elsewhere.

### Dependence on Global Supply Chains

Retailers rely on a continuous flow of goods and products, many of which are manufactured overseas and are shipped to the United States, making them vulnerable to supply chain interruption due to port closures, terrorist attacks, or natural disasters.

### Retail Stores as Distribution Centers during Disasters

Retail distribution centers, such as home improvement stores, supply key resources during disasters, and many response plans use shopping centers as distribution points, with the assumption these facilities will still be operational. During disasters, the Retail Subsector has played a role in information sharing and donating supplies, services, and money.

### Reliance on Point-of-Sale Cyber Systems

Retailers rely on point-of-sale cyber systems for financial transactions. These systems have been successfully attacked by hackers, and will likely continue to be targeted in the future.

## Sports Leagues Subsector

**Employment**
Supports over 133,000 jobs

**Economic Output**
Four major sports leagues produce $23B revenue

**Facilities**
Over 4,000 establishments across the United States

The subsector includes major sports leagues and federations. Over 4,000 establishments[38] related to spectator sports are spread across the United States, and the industry supports more than 133,000 jobs.[39] The four major sports leagues alone—National Football League, National Basketball Association, National Hockey League, and Major League Baseball—produce about $23 billion in revenue annually.[40]

The Sports Leagues Subsector is closely related to the Public Assembly Subsector. These facilities share many of the same characteristics, demographics, and, in many cases, owner–management relationships.

### Key Asset Considerations

#### Ownership/Owner–Lessee Agreements

In most situations, another entity (e.g., a local government or authority) owns the facility where sports teams hold their events. In many cases, these facilities are also considered multipurpose because other sporting events and different activities (e.g., trade shows, conventions, conferences, and concerts) are held in the same facility. Many of the large venues used in the four major sports leagues are also privately owned.

#### Emergency Shelters

Sports Leagues Subsector facilities may be designated as mega-shelters and used to house evacuees from a major disaster area, such as during wildfires or hurricanes. During an incident, facilities may also act as temporary shelter for displaced individuals or as an emergency services command center for local and Federal first responders.

#### Command Centers

Many sports league facilities with large attendance use a command center to monitor activities and to serve as an operations center in the event of a manmade or natural incident.

#### Security

For these facilities, security may be handled by local law enforcement, a private company, or a mixture of the two.

#### Support Anti-terrorism by Fostering Effective Technologies Act (SAFETY Act)

Established in 2002, the SAFETY Act created liability limitations for claims resulting from an act of terrorism where Qualified Anti-Terrorism Technologies have been deployed, encouraging antiterrorism programs and technology in stadium applications. Since 2008, the National Football League's Best Practices for Stadium Security, Major League Baseball's All Star Game, and several sporting venues have received SAFETY Act protections. Facilities in other subsectors have also received SAFETY Act protections, and the CF Sector is working to raise awareness among the whole sector.

# 2.2 Sector Risks

The CF Sector is one of the few U.S. critical infrastructure sectors in which terrorists have executed multiple high-profile attacks directly affecting the public, both in the physical and cyber domain. The following section covers emerging risks to the CF Sector and outlines the sector's risk profile.

## Notable Trends and Emerging Issues

- **Changing domestic and international terrorist threats—**The Boston Marathon bombing in 2013 highlighted the danger posed by homegrown violent extremists (HVEs)—lone actors or insular groups that are not directly tied to terrorist organizations. Federal counterterrorism experts consider HVEs to be "the most likely immediate threat to the homeland."[41] The United States also faces growing threats from the terrorist group Islamic State of Iraq and the Levant (ISIL), those it inspires, and other international terrorist groups. Insider threats—radicalized individuals who may work at a commercial facility and use their inside knowledge to exploit vulnerabilities—are also a growing concern.

- **Increasing interdependencies between sectors—**Cities and regions increasingly rely on complex networks of interconnected infrastructure that comprise and are operated by integrated physical and cyber systems. After a disaster, a failure in one system—such as in the Water or Energy Sectors, on which the CF Sector relies strongly—could cascade and greatly affect the regions they serve.

- **Increased cyber risks—**Adversaries have successfully executed point-of-sale attacks on large retailers and hotels to gain access to confidential data, which has cost companies and financial institutions hundreds of millions of dollars. Governments have launched targeted cyber espionage or sabotage attacks, and there has been an increase in "hacktivism," or politically motivated cyberattacks. The Federal Bureau of Investigation (FBI) identified North Korea as the source behind recent cyberattacks that published thousands of confidential company documents online, including personal email correspondences and employee data.[42] Building management systems—from heating, ventilation, and air conditioning (HVAC) systems, to access control—are increasingly computerized, making a growing portion of operations vulnerable to a cyberattack or information technology (IT) outage. Due to the CF Sector's dependency on the Internet and IT, the failure or infiltration of cyber systems would create a significant negative economic impact on the sector.

- **Increasing use of social media—**Social media sites allow people to immediately document and disseminate information, making it crucial for the CF Sector to respond to incidents quickly and efficiently. Social media brings both risks and benefits; for example, malicious actors could use social media to disrupt events, facilitate attacks, or organize flash mobs, but the sites may also contain valuable information that could aid security efforts during an event or recovery.

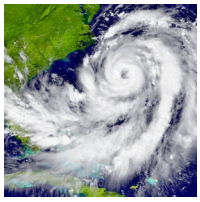
- **Emerging threats from the use of unmanned aircraft systems (UAS)—**The increased use of UAS, also called drones, and the absence of regulation is a growing threat for the CF Sector. These devices are of serious concern and can be used to cause damage to persons and property, as well as cause alarm at CF events or locations. Drones also allow individuals to gain access to previously unreachable areas, such as the air space above a stadium or movie studio, and could cause harm if armed with explosives.

- **Growing size and frequency of mass protests—**Social media is also facilitating "increasingly rapid, broad, and coordinated protest activities" at CF facilities. Protests can pose sanitation, public safety, economic, and other risks to CF occupants and guests.

## Significant Commercial Facilities Sector Risks

The sector operates through a principle of open public access and experiences high-population densities, which can increase the vulnerability to intentional attacks that aim to harm public health and safety, cause property damage, and inflict economic and psychological consequences. In addition, many venues are highly recognizable, increasing the potential attractiveness to an adversary. Below are the key risks affecting the security and resilience of CF Sector assets, operations, and workforce.

## Natural Disasters and Extreme Weather



Increasingly severe weather events, including storms, earthquakes, floods, and droughts, 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.

## 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.

## Pandemic

A pandemic could severely threaten the large workforce of CF Sector establishments, compromising facility operations or limiting services. Pandemics can also spread easily through CF facilities, as large groups of people congregate in them daily. This could have an economic effect on businesses if customers choose to stay home rather than risk infection. Many private businesses lack system-wide business continuity plans for catastrophic health emergencies. Plans must account for extreme health impact assumptions as well as containment.

## 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 footage, and result in the release of private information (e.g., customer credit card accounts, financial information, and internal correspondence).

## 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, particularly at outdoor events or facilities with limited screening, makes many facilities particularly vulnerable to explosives.

## Chemical, Biological, Radiological Attacks

Terrorist organizations have expressed interest in acquiring chemical, biological, or radiological (CBR) weapons, which can be widely dispersed through ventilation systems, food products, or liquids in an arena to inflict severe harm.

### Mass Protests

Although the majority of mass protests have been peaceful, some have resulted in property damage and can pose sanitation, safety, and other risks to building occupants and guests.

### Theft


CF Sector businesses are impacted by a range of theft-related crimes. For instance, organized theft of products and goods costs the Retail Subsector billions of dollars each year, and ATM-related thefts impact facilities in the Real Estate Subsector. Intellectual property theft threatens a company's ideas and inventions, including trade secrets, proprietary products, media, and software.

### Unmanned Aircraft Systems

Malicious actors could use UAS or drones to gain security knowledge or private information about a facility or event, which could provide information that could be used for attacks. Drones could also be used for intellectual property theft, such as recording over stadiums or movie studios, or could be armed with a deadly weapon to execute terrorist attacks from the air. This could cause serious damage to persons and property. The CF Sector is collaborating with the Federal Aviation Administration (FAA) to address drone safety and security.

### Supply Chain Disruptions

Incredibly efficient supply chains have resulted in a "just-in-time" delivery model—such as used in hotels and retail chains—that leaves companies with very limited inventories, making some firms highly sensitive to supply disruptions. If raw materials are unable to reach company facilities, it can disrupt operations or hinder disaster response. Likewise, if finished products are unable to be delivered, it can have a significant economic effect on companies. Supply chain disruptions could result from a range of causes, including geopolitical unrest, natural disasters, or tainted or counterfeit products being introduced into the manufacturing stream. Shipment tracking and management, in particular, may rely on the Global Positioning System and its precise positioning, navigation, and timing data. A data disruption could create cascading supply chain disruptions.

### Global Political and Social Implications

The CF Sector includes companies with international operations, such as global hotel chains, resorts, retail companies, and theme parks. These organizations need to keep informed of international threats, since maintaining the integrity of their brand and safety of their employees and patrons necessitates remaining aware of global risks.

## Primary Cross-Sector Interdependencies

The CF Sector is tightly integrated with other critical sector operations, which creates interdependencies that can cause a disruption in one sector to affect safe operations in another. CF Sector interdependencies include:


**Provides power**, which supports critical facility functions, such as lighting, water pumping, and HVAC systems. This is the primary dependency for the CF Sector. Without power, many facilities could not function for an extended period of time, as access to backup power is often limited in scope. An interruption to the power supply would directly affect all facilities located in the region serviced and could have cascading effects on other sectors that are dependent on goods provided by the affected commercial facilities.


**Provides a supply of potable water and handles the treatment of wastewater produced by the public.** The sector also provides water for fire suppression systems. Without these services, State or local health departments might shut down commercial facilities until services are restored.


**Saves lives and protects property after incidents**, such as accidents, natural disasters, or terrorist attacks. The CF Sector coordinates with Emergency Services—which includes law enforcement, fire and emergency services, and emergency medical services—to mitigate risk and respond to incidents. A disruption would affect the CF Sector's disaster response and prevention capabilities. Emergency Services also manages crisis reentry for affected areas, which is a critical issue for CF Sector owners and operators trying to gain access to their facilities.


**Provides telecommunications access and enables operations.** Damage to the Communications Sector would affect the CF Sector's ability to operate and could cause cascading economic damages as employees and customers may have difficulty communicating with the sector. Disruption to critical communications operations in facilities, such as stadiums or casinos, may hamper the sector's ability to respond to incidents.


**Provides the transportation of goods to and from commercial facilities, as well as the transportation of employees and customers during regular operations and after disasters.** A disruption in the Transportation Systems Sector could prevent employees or customers from reaching commercial facilities, or keep them from being able to leave facilities after an incident. A disruption could also keep goods and supplies from leaving or reaching the CF Sector. The CF Sector also needs to be able to gain access to areas after disasters to distribute resources to and reopen facilities.


**Enables day-to-day operations and financial transactions.** Loss of function would affect the sector's ability to operate, both for physical systems that have been automated and cyber systems.


**Provides services to the public** in the event of an attack, natural disaster, or pandemic/large-scale outbreak of an illness. Pandemics can spread easily through CF facilities as large groups of people congregate daily in CF facilities. Healthcare services are essential in the event of a disaster.


**Provides essential services** for the CF Sector to conduct daily business operations and emergency response, and is dependent on the CF Sector for business facilities. During disasters, CF facilities may house ATM and banking resources that the public will need to access during incidents.


**Resides within CF Sector properties as tenants or adjacent to commercial facilities.** This affects the risk of both sectors, which collaborate to address security challenges.


**Provides food and beverages served and sold in commercial facilities.** Many commercial facilities rely on restaurants located in their facilities (e.g., restaurants in malls and shopping districts), and fairs and festivals often feature special types of food and beverages. The CF Sector and Food and Agriculture Sector have also collaborated on food defense issues, such as the threat of malicious actors intentionally contaminating food products at commercial facilities.

# 2.3 Critical Infrastructure Partners

Voluntary collaboration between private sector and government stakeholders has been and remains the primary mechanism for advancing collective action toward national CF Sector security and resilience. Like all 16 critical infrastructure sectors, the CF Sector operates under the NIPP 2013 partnership structure, which provides the mechanisms to enable participation from the private sector; government partners at Federal, State, local, tribal, and territorial levels; and research and nongovernmental organizations that support sector security and resilience.

## Commercial Facilities Sector Partnership Structure

Figure 1. Commercial Facilities Sector Partnership Structure


The NIPP 2013 partnership structure includes representative public and private sector councils that operate under the Critical Infrastructure Partnership Advisory Council (CIPAC) construct. CIPAC facilitates interaction between the community of owners and operators and the sector's Federal, State, local, tribal, and territorial government representatives to conduct deliberations and form consensus positions for the Federal Government.

The CF Sector partnership includes the full community of private sector owners and operators, represented by members in eight subsectors on the Sector Coordinating Council (SCC). Key government partners are represented on the Government Coordinating Council (GCC). The partnership's success depends on the ability to leverage the full spectrum of capabilities and expertise from the sector through the activities of the partnership councils.

CF Sector partnership councils meet separately and during Joint Council meetings at least three times per year to facilitate sector-level planning; exchange information and lessons learned; establish effective coordinating structures; and develop security and resilience tools, guidelines, products, and programs. An updated list of council members and their charters can be found on the Commercial Facilities Sector Council Charters and Membership Webpage.

### Sector-Specific Agency

Sector coordination is led by DHS, which was designated as the Sector-Specific Agency (SSA). DHS serves as the primary Federal interface for sector-specific security and resilience efforts, promotes sector-wide information sharing, and supports implementation of the NIPP 2013 within the CF Sector.

The Office of Infrastructure Protection (IP) fulfills the role of SSA on behalf of DHS. The Assistant Secretary for IP chairs the CF GCC and has designated the Director of the Sector Outreach and Programs Division (SOPD) as the representative on behalf of IP. The Director designates an alternate to assist or act on behalf of the Director as necessary.

### Commercial Facilities Government Coordinating Council

The GCC enables interagency, intergovernmental, and cross-jurisdictional coordination on security and resilience strategies, activities, and policies. Members include Federal departments and agencies who coordinate with CF owners and operators and have a stake in sector security and resilience. State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) members also serve as liaisons to the CF GCC, representing SLTT perspectives at GCC and joint GCC-SCC meetings.

### Commercial Facilities GCC Members

- Government Services Administration
- U.S. Department of Agriculture
- U.S. Department of Health and Human Services
- U.S. Department of Homeland Security
- U.S. Department of Justice

## Commercial Facilities Sector Coordinating Council

The SCC is a self-organized, self-governed council of private sector asset owners and operators that coordinate on strategy, policy, information sharing, and risk management activities. Risk assessment and mitigation is primarily the responsibility of private sector owners and operators in the CF Sector. The sector has formed nine subcouncils of the SCC to facilitate information sharing and collaborative risk mitigation with industry peers—two within the Retail Subsector and one for each of the remaining subsectors. The SCC Executive Committee includes permanent, voting members from each of the nine subcouncils.

Through the partnership structure, the CF Sector also partners with organizations at all levels of government, regional organizations, international partners, and private sector owners and operators in other sectors.

### Commercial Facilities SCC Executive Committee Members

- Analytic Risk Solutions, LLC
- Beacon Capital Partners
- Bluegreen Vacations
- Boyd Gaming Corporation
- Contemporary Services Corporation
- Macerich
- Marriott International
- National Football League
- Peppermill Resort Spa Casino
- Real Estate Roundtable
- Sea World
- Simon Property Group
- Stadium Managers Association
- U.S. Tennis Association
- Venue Solutions Group, LLC
- Viacom

### Trade Associations

Trade associations, although not official members of the SCC, are a key mechanism to distribute information to sector partners they represent. Trade associations provide important feedback and input into CF Sector materials and activities. Partners include, but are not limited to:

- **American Gaming Association**—Works to create a better understanding of the gaming industry by bringing facts about the industry to the general public, elected officials, other decision-makers, and the media through education and advocacy.
- **American Hotel & Lodging Association**—The only U.S. association focused on the needs of every segment of the lodging industry.
- **American Resort Development Association**—Represents the vacation ownership and resort development industries (timeshares).
- **ASIS International**—The leading organization for security professionals, with more than 38,000 members worldwide.
- **Building Owners and Managers Association International**—Represents the owners and managers of all commercial property types including nearly 10 billion square feet of U.S. office space.
- **International Association of Amusement Parks & Attractions**—The largest international trade association for permanently situated amusement facilities worldwide.

- **International Association of Fairs & Expositions**—A voluntary, not-for-profit corporation serving State, provincial, regional, and county agricultural fairs, shows, exhibitions, and expositions.
- **International Association of Venue Managers (IAVM)**—Represents public assembly venues from around the globe. IAVM counts more than 500 companies among its members, including senior executives from auditoriums, arenas, convention centers, exhibit halls, stadiums, performing arts centers, university complexes, and amphitheaters.
- **International Council of Shopping Centers**—A leader in developing and maintaining high standards for shopping center professionals in a variety of areas, including security.
- **NAIOP: Commercial Real Estate Development Association**—Serves as the trade association for developers, owners, and investors in industrial, office, and related commercial real estate.
- **National Association of Theater Owners**—Represents roughly 32,000 movie screens in all 50 States and additional cinemas in 81 countries worldwide.
- **National Retail Federation**—Industry's largest advocacy organization, which advances the industry through professional seminars, trade conferences, publications, and educational activities.
- **Outdoor Amusement Business Association**—Promotes the preservation and growth of the outdoor amusement industry through leadership, advocacy, and education.
- **Real Estate Board of New York**—Unites more than 15,000 real estate professionals as it works to protect, improve, and advance the business of real estate in New York City.
- **Real Estate Information Sharing and Analysis Center (RE-ISAC)**—Public-private partnership between U.S. commercial facilities and the Federal Government to counter terrorism and protect buildings and the people who occupy and use them. Members include many of the aforementioned trade associations.
- **Retail Industry Leaders Association**—Provides a forum where members can conduct discussions aimed at understanding common operational practices, areas of concern, and pragmatic solutions to problems.

## Working Groups

The CF GCC and SCC have together developed working groups to create materials and programs designed to fill gaps and address security and resilience challenges identified by the sector. Each of the nine subsector councils has a working group. Additional working groups include:

- **Cybersecurity**—The Commercial Facilities Cybersecurity Working Group is a collaborative platform for all of the CF subsectors and facilitates the identification of long- and short-term cyber threats and vulnerabilities within the sector. The overarching goal is to provide a comprehensive hub for cybersecurity collaboration that brings cyber partners from across the CF Sector together to examine the ever-dynamic landscape of cyber threat, and to address that threat through a spectrum of activities—including formal and informal information sharing; the production of resources, products, and tools; and the creation of networking platforms.
- **Classified Intelligence Forum**—This forum provides appropriately cleared, identified partners with access to classified draft or finished intelligence products. By having cleared industry partners review drafts of finished intelligence and related products, DHS is able to obtain a better sense of what analysis the partners deem valuable.
- **Research and Development (R&D)**—The R&D Working Group includes representatives from each of the CF subsectors. It brings together owners and operators from the private sector to identify R&D gaps and serves as a platform for exploring feasible products and tools to solve those gaps.
- **Surveillance Awareness**—The CF Sector developed the Surveillance Awareness Working Group in response to growing partner needs related to surveillance detection with the goal of developing a Surveillance Awareness suite of projects. Through the working group, public and private sector partners address hostile surveillance methods and response.

# CHAPTER ENDNOTES


1. Developed using data from: U.S. Census Bureau, "Statistics of U.S. Businesses," NAICS codes 512, 515, 5111, 512131, 512132, accessed September 9, 2015, http://www.census.gov/econ/susb/.

2. Plunkett Research, Ltd., "Industry Statistics Entertainment & Media Business Statistics Analysis," last revised November 11, 2014, http://www.plunkettresearch.com/statistics/entertainment-media-publishing-market-research/.

3. American Gaming Association, 2013 *State of the States* (AGA 2013), http://www.americangaming.org/sites/default/files/aga_sos2013_rev042014.pdf.

4. American Hotel & Lodging Association, "2014 Lodging Industry Profile," accessed October 8, 2015, https://www.ahla.com/content.aspx?id=36332.

5. Developed using data from: U.S. Census Bureau, "Statistics of U.S. Businesses," NAICS codes 7132, 72112, accessed October 8, 2015, http://www.census.gov/econ/susb/.

6. International Association of Amusement Parks and Attractions, "Amusement Park and Attractions Industry Statistics," accessed October 8, 2015, http://www.iaapa.org/resources/by-park-type/amusement-parks-and-attractions/industry-statistics.

7. Developed using data from: U.S. Census Bureau, "Statistics of U.S. Businesses," NAICS codes 71, 7132, 71311, 72112 , 512131, 512132, accessed October 8, 2015, http://www.census.gov/econ/susb/.

8. U.S. Energy Information Administration, "2012 CBECS Preliminary Results," accessed October 8, 2015, http://www.eia.gov/consumption/commercial/reports/2012/preliminary/index.cfm.

9. Paul Emrath, "Multifamily Rental Properties: Would You Believe 2.25 Million?," Eye on Housing, March 29, 2013, accessed October 8, 2015, http://eyeonhousing.org/2013/03/multifamily-rental-properties-would-you-believe-2-25-million/.

10. Self Storage Association, "Fact Sheet," accessed October 8, 2015, http://www.selfstorage.org/ssa/Content/NavigationMenu/AboutSSA/Factsheet/default.htm.

11. Building Owners and Managers Association International, *Where America Goes to Work: The Contribution of Office Building Operations to the Economy*, 2012 (BOMA 2012), http://www.boma.org/industry-issues/state-local-issues/Documents/2011_BOMA_Econ_Impct_FINAL%20Proof%20for%20print.pdf.

12. Developed using data from: U.S. Census Bureau, "Statistics of U.S. Businesses," NAICS code 53, accessed October 8, 2015, http://www.census.gov/econ/susb/.

13. National Retail Federation, 2013 *Annual Report* (NRF, 2013), https://nrf.com/annualreport2013/PDFs/nrf-FINAL-pn-lowres.pdf.

14. Attendance data developed using these sources:
    - ESPN, "MLB Attendance Report—2014," accessed October 8, 2015, http://espn.go.com/mlb/attendance/_/year/2014.
    - ESPN, "NBA Attendance Report—2014," accessed October 8, 2015, http://espn.go.com/nba/attendance/_/year/2014.
    - ESPN, "NFL Attendance—2014," accessed October 8, 2015, http://espn.go.com/nfl/attendance.
    - ESPN, "NHL Attendance Report—2013-2014," accessed October 8, 2015, http://espn.go.com/nhl/attendance/_/year/2014.

15. Plunkett Research, Ltd., "Sports Industry, Teams, Leagues & Recreation Market Research," accessed October 8, 2015, http://www.plunkettresearch.com/statistics/sports-industry/.

16. Plunkett Research, Ltd., "Entertainment, Media, Publishing & Broadcasting Industry Market Research," accessed October 8, 2015, http://www.plunkettresearch.com/entertainment-media-publishing-market-research/industry-and-business-data.

17. Federal Communications Commission, *Broadcast Station Totals as of June 30, 2014* (FCC, 2014), https://apps.fcc.gov/edocs_public/attachmatch/DOC-328096A1.pdf.

18. National Association of Broadcasters, "Frequently Asked Questions About Broadcasting," accessed October 8, 2015, http://www.nab.org/documents/resources/broadcastFAQ.asp.

19. Motion Picture Association of America, "Creating Jobs," accessed October 8, 2015, http://www.mpaa.org/creating-jobs/.

20. American Gaming Association, "Groundbreaking New Research Reveals Impressive Magnitude of U.S. Casino Gaming Industry,"accessed October 8, 2015, http://www.gettoknowgaming.org/news/groundbreaking-new-research-reveals-impressive-magnitude-us-casino-gaming-industry.

21. National Indian Gaming Commission, "Media teleconference: 2013 Indian Gaming Revenues Increased 0.5%," July 18, 2014, http://www.nigc.gov/LinkClick.aspx?fileticket=vQueScguAW8%3d&tabid=1006.

22. Ibid.

23. U.S. Travel Association, *Travel Exports: Driving Economic Growth and Creating American Jobs* (U.S. Travel Association, 2014), https://www.ustravel.org/sites/default/files/page/2009/09/2014_Export_Report-PDF-FINAL.pdf.

24. SelectUSA, "The Travel, Tourism and Hospitality Industry in the United States," accessed October 8, 2015, http://selectusa.commerce.gov/industry-snapshots/travel-tourism-and-hospitality-industry-united-states.

25. American Hotel & Lodging Association, "2014 Lodging Industry Profile," accessed October 8, 2015, http://www.ahla.com/content.aspx?id=36332.

26. International Association of Amusement Parks and Attractions, "Amusement Park and Attractions Industry Statistics," accessed October 8, 2015. http://www.iaapa.org/resources/by-park-type/amusement-parks-and-attractions/industry-statistics.

27. Ibid.

28. Jessie Durando, "Traditions: Macy's Thanksgiving Day parade explained," USA Today, February 23, 2015, http://www.usatoday.com/story/news/nation-now/2014/11/24/thanksgiving-traditions-macys-parade/19364279/.

29. Plunkett Research, Ltd., "Entertainment, Media, Publishing & Broadcasting Industry Market Research," last revised November 24, 2014, http://www.plunkettresearch.com/entertainment-media-publishing-market-research/industry-and-business-data.

30. American Alliance of Museums, "Museum Facts," accessed October 8, 2015, http://www.aam-us.org/about-museums/museum-facts.

31. Association of Zoos and Aquariums, "Zoo and Aquarium Statistics," accessed October 8, 2015, https://www.aza.org/zoo-aquarium-statistics/.

32. National Multifamily Housing Council, "Quick Facts: Resident Demographics," accessed October 8, 2015, http://www.nmhc.org/Content.aspx?id=4708#What_type_of_structure.

33. The Real Estate Roundtable, "Continuing the Effort to Restore Liquidity in Commercial Real Estate Markets," accessed October 8, 2015, http://www.rer.org/uploadedFiles/RER/Policy_Issues/Credit_Crisis/2009_09_Restoring_Liquidity_in_CRE.pdf?n=8270.

34. Building Owners and Managers Association (BOMA) International, *Where America Goes to Work: The Contribution of Office Building Operations to the Economy*, 2012 (BOMA, 2012), http://www.boma.org/industry-issues/state-local-issues/Documents/2011_BOMA_Econ_Impct_FINAL%20Proof%20for%20print.pdf.

35. Self Storage Association, "Fact Sheet," accessed October 8, 2015, http://www.selfstorage.org/ssa/Content/NavigationMenu/AboutSSA/Factsheet/default.htm.

36. National Retail Federation, 2013 *Annual Report* (NRF, 2013), https://nrf.com/annualreport2013/.

37. Forrester Research, Inc., "US Online Retail Sales to Reach $370 Billion by 2017," accessed October 8, 2015, https://www.forrester.com/US+Online+Retail+Sales+To+Reach+370+Billion+By+2017/-/E-PRE4764.

38. Developed using data from: U.S. Census Bureau, "Statistics of U.S. Businesses," NAICS code 7112, accessed October 8, 2015, http://www.census.gov/econ/susb/.

39. United States Department of Labor, "May 2013 National Industry-Specific Occupational Employment and Wage Estimates," accessed October 8, 2015, http://www.bls.gov/oes/current/naics4_711200.htm.

40. Plunkett Research, Ltd., "Sports Industry, Teams, Leagues & Recreation Market Research," accessed October 8, 2015, http://www.plunkettresearch.com/statistics/sports-industry/.

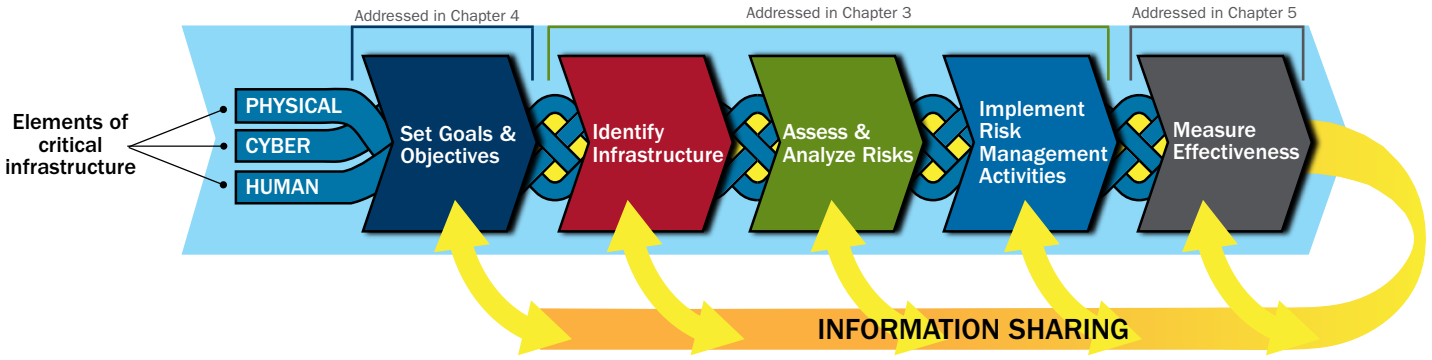
41. National Counterterrorism Center, *Cyber Security, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland* (NCTC, 2014), http://www.nctc.gov/docs/cyber_security_terrorism_and_beyond.pdf.

42. Nicholas J. Rasmussen, Director, National Counterterrorism Center, "Current Terrorist Threat to the United States," Hearing before the Senate Select Committee on Intelligence, February 12, 2015, http://www.nctc.gov/docs/Current_Terrorist_Threat_to_the_United_States.pdf; The Federal Bureau of Investigation, "Update on Sony Investigation," December 19, 2014, accessed October 8, 2015, https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

# 3 RISK MANAGEMENT AND NATIONAL PREPAREDNESS

Risk management is the cornerstone of the NIPP 2013 and the national effort to strengthen security and resilience. It enables owners and operators to make risk-informed decisions that best allocate limited resources to the most effective mitigation solutions. The NIPP 2013 outlines a risk management framework that enables the critical infrastructure community to focus on those threats and hazards that are likely to cause harm, and employ prioritized approaches that are designed to prevent or mitigate the effects of those incidents. It also increases security and strengthens resilience by identifying and prioritizing actions to ensure continuity of essential functions and services during incidents and supports rapid response and restoration. For more information on sector resources, visit the Commercial Facilities Sector Webpage or email CFSTeam@hq.dhs.gov.

Figure 2. NIPP 2013 Critical Infrastructure Risk Management Framework




The CF Sector goals and priorities are directly rooted in the NIPP 2013 risk management framework. Updated goals and priorities reflect the maturation of the partnership and the significant progress made toward the 2010 Sector-Specific Plan (SSP). This section presents the sector's ongoing efforts and the planned approaches that support risk management and national preparedness, response, and recovery following an incident that affects CF Sector operations.

## 3.1 Risk Management

Under the NIPP 2013 framework, risk is the potential for an adverse outcome from an event, determined by the event's likelihood—a function of the specific threats and vulnerabilities—and associated consequences if the event occurs.[43] Although individual owners and operators are responsible for managing risk to their individual assets, CF Sector partnership activities can improve understanding of threats, vulnerabilities, and consequences and provide owners and operators with tools, guidelines, information, best practices, and resources to facilitate more effective risk assessments and risk management decisions at the facility and sector level.

Owners and operators in the CF Sector assess individual risks and establish internal plans to mitigate risks and respond to disruptions. They also work collaboratively with sector partners to conduct vulnerability assessments of high-priority infrastructure; participate in DHS-sponsored CF Webinars, threat briefings, and training; and collaborate with State, local, and regional authorities to build disaster response.

The following subsections identify the general ways in which CF subsectors mitigate risk in accordance with the NIPP 2013.

### Identify Infrastructure

Each subsector—through associations and/or individual business practices—identifies and prioritizes its most critical assets and targets collaborative risk mitigation activities to address those assets with a high risk profile. Owners and operators also work closely with State and local partners to identify regionally critical assets and contribute to regional disaster response planning to ensure the continuity of those assets. The primary characteristics that influence prioritization of assets include an asset's iconic importance, location and proximity to high-risk enterprises, financial importance, size, and number of employees and visitors.

## Assess and Analyze Risks

Facility-specific cyber and physical risk assessments examine the individual vulnerabilities and local and regional consequences of a facility disruption, factoring in relevant information about CF Sector threats from operational experience and intelligence information sharing. These assessments help owners and operators identify the specific security and resilience measures that would best reduce risk and prioritize security spending.

Concern over public disclosure plays a significant role in determining what information about individual vulnerability assessments SCC members will provide to government partners. However, they frequently work with Federal, State, and local government agencies to leverage partner resources in conducting risk assessments for high-value facilities that contribute to regional or national security and resilience.

DHS has provided strategic coordination and field operations support to assist owners and operators with risk assessments, such as the **Computer-Based Assessment Tool** (CBAT). Over 360 CBATs have been conducted in the CF Sector since 2006.

**RISK ASSESSMENT**

CF Sector risks can be assessed at the facility and sector level as a function of threats, vulnerabilities, and consequences associated with a particular event. Criteria that may be considered include:

**Threat**
Natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

**Vulnerability**
Physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.

**Consequence**
Effect of an event, incident, or occurrence.

DHS also participates in several information-sharing programs to inform and engage with owners and operators and to allow facilities to report suspicious activity and threat information.

The **Classified Intelligence Forum** is a pilot program for the CF Sector in which sector representatives sit alongside I&A analysts to review intelligence, provide analysis for the information's impact on the sector, and inform and advise the U.S. Government on intelligence products. The program provides appropriately cleared, identified members of CIPAC with access to classified draft or finished intelligence products. This allows I&A analysts to solicit feedback and gain overall customer insights that inform the development of products and briefings, allow for the dissemination of materials, and produce other support that members and their sector constituents can use in security decision-making processes. By having cleared industry partners review drafts of finished intelligence and related products, DHS is able to obtain a better sense of what analysis the partners deem valuable. In turn, I&A analysts develop additional products that are better tailored to partners' information and intelligence needs.

DHS also conducts **briefings** and **teleconferences** to address event-specific threats, either to review lessons learned or raise awareness of emerging threats. Past sessions have included a teleconference over lessons learned in the response and preparation for Superstorm Sandy; two unclassified threat briefings to the National Association of Theater Owners in the aftermath of the Aurora, CO, theater shooting; outreach within major metropolitan areas regarding social media and emerging threats; and 78 facilitated discussions and exercises with the FBI and retail partners in response to the Nairobi, Kenya, Westgate shopping mall attack.

DHS and the FBI work together to increase sector awareness of risks. For example, DHS and the FBI issue **Joint Special Assessments** and **Joint Information Bulletins** to members of the Entertainment and Media, Gaming Facilities, Public Assembly, and Sports Leagues Subcouncils. These address possible terrorist activities related to each of the subsectors. Private sector members of all CF subcouncils also work to develop relationships with the FBI, and the FBI also partners with DHS to offer training, exercises, and workshops.

The **RE-ISAC** serves as a conduit for disseminating threat information from the public sector to the private sector and collects threat information from the private sector for analysis by Homeland Security officials across the CF Sector. The RE-ISAC also brings together private and public sector experts to share useful information and to discuss and develop best practices and solutions on subsector-specific issues. These include issues affecting retail or office property owners and cross-sector issues, such as risk assessment, daily reports, asset fortification/hardening, cyber and physical security, and emergency-response planning.

A **Suspicious Activity Reporting Tool** provides a means for critical infrastructure partners to use sector sites on Homeland Security Information Network-Critical Infrastructure (HSIN-CI) to report suspicious or unusual activities to the government. Since 2011, partners have submitted 24 of these reports.

**Fusion centers** serve as primary focal points at the State and local level for the receipt, analysis, gathering, and sharing of threat-related information among Federal and State, local, tribal and territorial (SLTT) and private sector partners. The centers include Federal interagency partners such as DHS, the FBI, and the Department of Justice (DOJ). In certain regions, CF Sector owners and operators work closely with fusion centers to share two-way threat information and ensure effective analysis of intelligence for use in the CF Sector. For a list of fusion centers and their contact information, please see the National Fusion Center Association Website.

**Protective Security Advisors** (PSAs), operating under IP, also provide owners and operators with critical information. PSAs have five mission areas: plan, coordinate, and conduct security surveys and assessments; plan and conduct outreach activities; support NSSEs and Special Event Activity Rating (SEAR) Level 1 and Level 2 events; respond to incidents; and coordinate and support IED awareness and risk mitigation training. PSAs also conduct Enhanced Critical Infrastructure Protection (ECIP) visits to inform and educate owners and operators on threats from terrorism, the criticality of their facilities, and available IP and DHS resources. Over 2,200 ECIPs have been conducted with CF partners. For more information or to contact your local PSA, please send an email to PSCDOperations@hq.dhs.gov.

**Infrastructure Survey Tool** (IST) security surveys are Web-based tools that allow DHS to identify and document overall critical infrastructure security, provide information for protective measures planning and resource allocation, facilitate government information sharing, and enhance its ability to analyze data and to produce improved metrics. The tool uses the **Protective Measures Index** methodology to measure the ability of a critical infrastructure asset to resist a disruptive event. IST includes a dashboard that creates a facility Protective Measures Index that can be used to compare against similar facilities; incorporates a **Resilience Measurement Index** (RMI) that is an aggregate measure of four components—preparedness, mitigation measures, response capabilities, and recovery mechanisms—and informs protective measures planning and resource allocation. The RMI, which ranges from 0 (low resilience) to 100 (high resilience), allows for comparison of the resilience of different critical infrastructure assets and provides a basis for prioritizing the implementation of operational and physical enhancements to increase asset resilience. Over 730 ISTs have been conducted. For more information about the Protective Measures Index, please send an email to PSCDOperations@hq.dhs.gov.

## Implement Risk Management Activities

On a collaborative basis, CF Sector partners work with the SSA to develop guidance and training that supports security and resilience, participate in voluntary programs that increase resilience, and engage in partnerships that improve information sharing and access to important resources.

As the CF SSA, DHS has worked extensively with subsector councils and has developed working groups (see Section 2.3 for full list) to create materials and programs designed to fill the gaps identified by the sector. The working groups bring together SCC members with experts outside the CF Sector. For example, the CF SSA developed a working group made up of the Emergency Services Sector SSA, representatives of the law enforcement community, and retail partners to develop guidance materials for the *Active Shooter: How to Respond* awareness initiative. The Retail Subsector spurred the creation of this content after identifying a gap in the educational materials that address the threat of an active shooter in a public place.

Owners and operators work directly with their peers through **private sector associations** that enable subsector collaboration on relevant security and policy issues. DHS typically works through these associations to **distribute information** directly to facilities and to contribute to the operation of the RE-ISAC (see full structure and partner list in Section 2.3). One example of how this works is through the **Real Estate Roundtable**, which brings together private and public institutions with a major national influence to communicate and collaborate on relevant national policy issues. The Real Estate Roundtable maintains a Homeland Security Task Force, which champions the sector's relationship with DHS and helps deliver relevant information from DHS to its members. The task force also serves as the CF Sector's official Real Estate Subsector Council. A selection of other private sector associations include the **American Gaming Association**, **Building Owners and Management Association**, **Retail Industry Leaders Association**, the **National Retail Federation**, the **International Shopping Council of Shopping Centers**, and **American Hotel and Lodging Association**. Many of these industry associations also contribute to the funding and operation of the RE-ISAC.

The 2002 **SAFETY Act** created liability limitations for claims resulting from an act of terrorism where the facility had deployed Qualified Anti-Terrorism Technologies. Commercial facilities—particularly in the Sports Leagues, Real Estate, and Retail Subsectors—have actively deployed new security technologies and received SAFETY Act protections. The CF Sector is working to raise awareness of the SAFETY Act and encourage greater participation in the sector as a whole.

The **Domestic Security Alliance Council**—a partnership between the U.S. Government and U.S. private industry—also advances the ability of owners and operators to protect employees, assets, and information. The council provides ongoing access to security information, a network of security experts, newsletters and bulletins, and continuing education for corporate Chief Security Officers and Intelligence Analysts.

Additionally, owners and operators have access to HSIN-CI, a source of threat information and materials—such as guidance, training, and planning tools—that DHS IP has developed with significant coordination from CF Sector owners and operators (for a full list, see Appendix C):

- The CF Sector published **Protective Measure Guides** for the lodging industry, commercial real estate, mountain resorts, and outdoor venues. These provide an overview of threat, vulnerability, and protective information to educate businesses as they consider implementing security measures in their facilities.
- Interactive, no-cost **online training** covers topics such as active shooter preparedness, insider threats, surveillance awareness, and more. Other courses include **Retail Security Awareness—Understanding Hidden Hazards, Surveillance Awareness: What You Can Do**, and **Bombing Prevention Training**.
- **Active shooter materials** include an online training course, desk reference guide, reference poster, and a pocket-size reference card addressing how managers, employees, and human resources operatives should train for and respond to an active shooter in their facility. Printed materials are available in both English and Spanish.
- **Pandemic Influenza Planning Materials** provide a suite of documents to enhance pandemic operational response planning.
- **Sector-Specific Tabletop Exercise Program for the Commercial Facilities Sector** allows users to leverage pre-built exercise templates and tailor them to a community's specific needs in order to assess, develop, and update plans, programs, policies, and procedures within an incident management functional area.
- **Videos** help to raise awareness of threats and risk management techniques, including:
    - **Check It!**, which provides information to help employees properly search bags in order to protect venues and patrons across the country;
    - **No Reservations: Suspicious Behavior in Hotels**, which provides information to help employees identify and report suspicious activities and threats in a timely manner; and
    - **What's in Store: Ordinary People/Extraordinary Events**, which provides information on identifying and reporting suspicious activity and threats at shopping centers and retail establishments.
- **Webinars** allow owners and operators to improve response plans and better understand risks. Past topics include IED threat awareness and detection, evolving threats, hotel security, retail security, and surveillance detection.

**Tabletop exercises** allow owners and operators to gain additional insight into how to promote resilience. For example, one past information-sharing tabletop exercise included facilitated discussions for all the CF subsectors. Representatives from the subsectors, as well as representatives with the Federal Government, reviewed the steps subsectors would take during an incident. Tabletop exercises can also focus on interdependencies between sectors by examining how a single event can cascade to cause multiple disruptions and affect lifeline sectors. After-action reports (AARs) typically provide concrete analysis of exercises and next steps to improve resilience.

Individual owners and operators participate in **information sharing with State, local, and regional partners**. This includes regular information sharing of ongoing risks and event-specific support and communication. For instance, the vice presidents of major gaming companies meet with local law enforcement, State partners, and PSAs on a monthly basis, and companies from the Entertainment and Media Subsector regularly meet with the Los Angeles Police Department and Los Angeles Sheriff to exchange threat information. Local law enforcement may also support security for the Sports Leagues Subsector, and sporting events with national recognition may also involve the support of the U.S. Secret Service,

U.S. Immigrations and Customs Enforcement, and others. This information sharing also allows facilities to assess regional interdependencies and to prepare for disaster response. For example, after a natural disaster, stadiums and hotels may serve as temporary housing facilities. The CF Sector's private partners expressed the need to expand on existing coordination with local and regional partners to improve disaster response.

CF Sector private security directors report that **personal relationships** are paramount for effective information sharing and frequently serve as their primary source of threat information. Security directors often leverage both formal and informal information channels to share and validate information. Many directors noted that when they receive government information through a security bulletin or other formal channel, they often reach out to their personal contacts in the appropriate agency to validate, clarify, or augment the information. Personal contacts are equally important at the local level, where security directors are in close contact with State and local law enforcement for incident response and suspicious activity reporting. One focus of the CF Sector over the next four years—reflected in activities noted in Section 4.1—is to formalize these personal relationships and to streamline information sharing from multiple channels.

## 3.2 Managing Cyber Risks

The CF Sector widely uses Internet-enabled systems for marketing, merchandising, ticketing, and reservations. As a result, owners and operators manage and protect enormous databases of customer data, including personal, financial, and credit card information. A large communications failure or intentional cyberattack could substantially disrupt payments and basic operations, compromise customer and company data privacy, threaten company integrity and reputation, and create large legal and economic burdens. A sophisticated cyberattack could also potentially give hackers access to or control of automated building systems, including electronic security, access control, and internal surveillance.

Recent high-profile cyber breaches at major retail and media companies have highlighted the growing capabilities of cyber adversaries and sizable economic consequences of cyberattacks. Owners and operators typically manage cybersecurity issues on an individual basis or with a few key partners. However, cybersecurity risks and trends, when taken collectively, often reach levels of scope and complexity that fall beyond the ability of individual industries and government organizations to manage.

CF Sector partners rely on their industry peers and government partners to share information on sector-level cyber risks, imminent cyber threats, and cybersecurity best practices. In the CF Sector in particular, these resources include the following:

- The RE-ISAC, as a primary conduit of cyber risk information to the CF Sector, shares sector-relevant cyber information from across government sources, including fusion centers, the United States Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).
- The *Cybersecurity in the Retail Sector* Webinar provides retail employees and managers with an overview of the cyber threats and vulnerabilities facing the industry. It also reviews the types of cyber systems and infrastructure used by the retail industry and what retail personnel can do to address the industry's unique vulnerabilities to those cyber resources.
- The CF Sector launched its Cyber Working Group in 2014 to gain better insight into private sector cybersecurity needs and practices and to promote implementation of the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Through the Cyber Working Group, the CF Sector has begun to work closely with the DHS Office of Cybersecurity and Communications (CS&C) to support the Critical Infrastructure Cyber Community ($C^3$) Voluntary Program—the coordination point within the Federal Government for critical infrastructure owners and operators interested in improving their cyber risk management processes. CS&C and the CF Sector are working together to improve cyber resilience in several ways:

- The CF Sector shares information about the $C^3$ program to its members, including by promoting the $C^3$ website, outreach materials, and workshops around the country.
- In 2013, the CF SSA identified its critical cybersecurity functions and services as part of the Cyber-Dependent Infrastructure Identification (CDII) effort, called for by EO 13636. This effort resulted in sector critical functions validated by industry subject matter experts (SMEs). As a result, the CF Sector is positioned to conduct a sector-wide cyber risk assessment leveraging the critical functions and services identified through the CDII effort.

- The Cyber Working Group, other sector organizations, and industry SMEs plan to work with DHS CS&C to evaluate the cybersecurity threats, vulnerabilities, and consequences to critical functions to establish the sector's cyber risk priorities. The CF Sector plans to work with CS&C to develop a long-term work plan and timeline for conducting a sector-wide cyber risk assessment.

In addition to these activities, CF Sector owners and operators have access to a number of tools, developed by CS&C, which can be used to assess cybersecurity capabilities and prioritize improvements:

- The Cybersecurity Evaluation Tool (CSET) is a no-cost product that offers a systematic and repeatable approach for organizations to assess the security posture of their cyber systems and networks.
- The Cybersecurity Evaluation Program and Cyber Resilience Review (CRR) is a no-cost, non-technical, and voluntary assessment for organizations to measure cybersecurity capabilities against the following ten domains: asset management, controls management, configuration and change management, vulnerability management, incident management, service continuity management, risk management, external dependency management, training and awareness, and situational awareness.

## 3.3 Mitigating Disruptions from the Loss of Lifeline Functions

The CF Sector is dependent on essential services provided by the Energy Sector, Water Sector, and Communications Sector. Without these services, the CF Sector would not be able to sustain operations. CF Sector owners and operators develop contingency plans, backup power and water sources, and alternate communication methods and transportation routes as part of their emergency operations and business continuity planning. In particular, owners and operators draw upon lessons learned from cross-sector partners during Federal, State, and local emergency and tabletop exercises to form more accurate expectations of lifeline function availability during a major disaster. For a more detailed description of interdependencies, please see the sector snapshot and Section 2.2.

Addressing critical interdependences requires active engagement and information sharing with cross-sector security partners to identify complementary risk management practices and programs that can improve local and regional resilience and mitigate consequences of loss of lifeline functions. Four of the CF Sector activities specifically focus on further addressing critical sector interdependencies:

- **Activity 15:** Work with the lifeline sectors, particularly the Energy and Water sectors, to examine strategies to sustain CF Sector operations during an interruption of services, such as by holding joint exercises, creating cross-sector councils, identifying ideas to improve resiliency, or organizing other activities.
- **Activity 16:** Work with the Emergency Services Sector and local officials to develop and conduct outreach for low-cost, unified, and nationwide response efforts—such as crisis reentry credentialing to ensure access to restricted areas after a disaster.
- **Activity 18:** Collaborate with the Financial Services Sector to create a joint resource for logging the accessibility of ATM and banking resources during disasters, leveraging the Financial Services Information Sharing and Analysis Center and Real Estate Information Sharing and Analysis Center.
- **Activity 24:** Build on the Resilience Measurement Index to establish a resilience "score card" that helps owners and operators in the CF Sector and lifeline sectors determine how resilience is being measured and managed, and assists government agencies with tracking their effectiveness in information sharing.

## 3.4 Research and Development Priorities

R&D activities are critical for developing novel technologies and methods to better assess and mitigate risks to CF Sector assets, systems, and networks. There are many cross-cutting R&D efforts, not only within DHS, but also within Federal agencies, academia, and international initiatives. As the CF SSA, DHS informs private sector partners of the latest developments in the sector's R&D portfolio.

The CF Sector has an R&D Working Group, which includes representatives from each of the CF subsectors. In fiscal year 2014, the R&D Working Group identified the top R&D needs for the sector. While many of these R&D needs have existed since the 2010 SSP, they will receive renewed attention with the publication of the 2015 *National Critical Infrastructure Security and Resilience Research and Development Plan* (CISR R&D Plan). The R&D Working Group has identified these efforts as top R&D needs for the CF Sector:

- **Integrated, Wide-Area Explosive and CBR Detection Devices—**The CF Sector is seeking to quickly and effectively detect and alert against chemical/biological/radiological/explosive (CBRE) hazards inside and outside of commercial facilities, including large numbers of people and large volumes of vehicles, trucks, and delivery items. The CF Sector is also seeking HVAC systems with CBR detection capability.
- **Image Recognition Systems (Identification, Verification, and Cross-Referencing Capabilities)—**A need exists for Image Recognition Systems that build on biographic and biometric collection and allow for real-time automated identification, verification, and cross-referencing with suspected terrorist watch lists. Current image recognition systems are not widely available and do not allow for real-time operations and automated identification, verification, and cross-reference with suspected terrorist lists.
- **Uniform Blast Effects Tool for Buildings and Facilities—**Current research activities are focused on blast dynamics in urban canyons (i.e., areas where streets cut through dense blocks of structures, causing a canyon effect). Research on the urban canyon model is important for downtown properties; however, many commercial facilities are not located in a metropolitan environment. Therefore, it is unclear whether this research and these tools would be applicable or would satisfy the needs of those types of properties. A tool that accommodates a variety of structural configurations in a variety of environments is needed.
- **Modeling, Simulation, and Strategies to Address the Handling and Evacuation of Large Crowds—**This gap addresses modeling and simulations to further refine strategies for quickly evacuating large crowds (e.g., 50,000 to 130,000 individuals).
- **Modeling and Analysis Study of the Economic, Social, and Political Impacts of Major Incidents—**A modeling and analysis study of the economic, social, and political impacts of a major natural disaster and a major terrorist attack against commercial assets would provide the necessary information to fill the recognized gap.
- **Inconspicuous Screening Technology—**Facilities within the CF Sector, such as stadiums and performance venues, need to balance security needs with positive customer perception. Developing technologies that can assist in less invasive and more aesthetically pleasing screening apparatus/equipment specifically for humans and baggage and seeking non-obtrusive and non-disposal technologies for explosive screening will help the CF Sector meet this need.
- **Create Next-Generation Explosive Detection Technologies/Methodology—**There is an R&D need to improve explosive detection capabilities and software lowering false alarm rates while increasing detection and throughput. Additionally, increased knowledge and analysis of these two areas would improve IED prevention and response: current U.S. counter-IED capabilities and practices for critical infrastructure facilities leading to recommendations for strengthening capabilities and practices against potential attacks.
- **Improve Ability to Detect, Assess, and Respond to Physical and Cyber Threats—**In order to raise the CF Sector's resilience, R&D should focus on improving analytical capabilities and increasing an interoperable distributed capacity to conduct, identify, and quantify cascading effects and indirect effects associated with cross-sector and cyber interdependencies under compound threat scenarios. This would include identifying the potential functional effects of cybersecurity failures in the sector and recognizing and assessing feasible scenarios where cyber or physical attackers prepare a geographically distributed attack against multiple critical infrastructure sectors, either as an isolated, coordinated assault or in combination with natural hazards. Additionally, R&D should contribute to increased knowledge on potential negative effects to critical cyber-physical systems by electronic emission employed by security assets, adversaries, and severe weather events, and the capabilities needed to mitigate those effects.

Cross-sector R&D needs were also identified in the CISR R&D. As part of the NIPP partnership structure, critical infrastructure sectors identify R&D priorities that require the resources and expertise of both public and private sector partners. These include:

- Develop the foundational understanding of critical infrastructure systems and systems dynamics.

- Develop integrated and scalable risk assessment and risk management approaches.
- Develop integrated and proactive capabilities, technologies, and methods to support secure and resilient infrastructure.
- Harness the power of data sciences to create unified, integrated situational awareness and to understand consequences of system failures and resulting cascading issues.
- Build a crosscutting culture of critical infrastructure security and resilience R&D collaboration to foster cross-sector involvement and dialogue.

The CF Sector plans to work closely with its Federal partners as part of CISR R&D plan and R&D Working Group implementation.

## 3.5 Commercial Facilities Sector National Preparedness Efforts

The five National Planning Frameworks—established under the National Preparedness Goal, the cornerstone for implementation of Presidential Policy Directive (PPD) 8: National Preparedness—foster a shared understanding of roles and responsibilities across critical infrastructure sectors to **prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk**. The previous sections of this SSP outlined the CF Sector's methods and measures for prevention, protection, and mitigating risk. The following section focuses on the role the CF Sector plays in response and recovery efforts after disasters.

The Emergency Support Function (ESF) structure under the National Response Framework outlines the coordination of Federal interagency support for a Federal response to an incident. Likewise, the Recovery Support Functions (RSFs) under the National Disaster Recovery Framework provide context for how partners work together to restore, redevelop, and revitalize the health, social, economic, natural, and environmental fabric of communities after events. The CF Sector plays a support role to other partners and agencies who lead emergency response and recovery by ensuring the resilience of their individual facilities, and by providing facilities with resources to critical infrastructure partners to support local and regional recovery efforts. A CF Sector operator can confirm that the facility is able to respond and recover, but must rely on the effectiveness and capabilities of regional lifeline services and local governments. The following are examples of how the CF Sector contributes to national response and recovery efforts:

- Hotels and motels—from the **Lodging Subsector**—are used as shelters during times of natural disasters, and hotel companies have collaborated to find rooms for disaster victims and to make their properties available in times of need.
- **Public Assembly Subsector** facilities provide extended shelter and comfort for displaced individuals after national disasters. These facilities may also provide temporary shelter for displaced individuals or serve as emergency services command centers for local and Federal first responders.
- **Sports Leagues Subsector** facilities may be designated as mega-shelters and used to house evacuees from a major disaster area. These facilities may also act as temporary shelter for displaced individuals or as an emergency services command center for local and Federal first responders.
- The **Real Estate Subsector** may work with the GSA in order to coordinate the advance provision of Joint Field Offices—where the Federal Emergency Management Agency (FEMA) coordinates disaster response and recovery efforts in areas affected by disasters.
- Many response plans use the **Retail Subsector** as distribution points. The sector has proven to be important in disaster response by sharing information and donating supplies, services, and money.

## CHAPTER ENDNOTES

43. DHS Risk Lexicon, 2010 Edition, https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf. Also referenced in the NIPP 2013.

# 4 VISION, GOALS, AND PRIORITIES

An effective CF Sector partnership is instrumental in achieving a vision shared by owners and operators and their government and community partners. The CF Sector GCC and SCC collectively developed five joint goals for sector security and resilience and seven priorities they will pursue over the next four years. These goals and priorities directly support the CF Sector risk management framework and approaches detailed in Chapter 3.

## COMMERCIAL FACILITIES SECTOR VISION

The CF Sector envisions a secure, resilient, and profitable sector in which effective and non-obstructive risk management programs instill a positive sense of safety and security among the public and patrons and sustain favorable business environments conducive to attracting and retaining employees, tenants, and customers.

Table 1. Commercial Facilities Sector Goals and Priorities

| Goals | Priorities | |
|---|---|---|
| 1 Strengthen trusted and protected information sharing and ensure sector access to timely, actionable, and threat-specific information and analysis. | PRIORITY A | Improve formal public-private information-sharing processes at all levels; expand owner and operator access to relevant intelligence; and centralize two-way, public-private threat sharing to streamline reporting. |
| | PRIORITY B | Promote value of participation in the sector partnership to better engage and reach out to all subsectors, smaller owners and operators, and industry organizations in the sector partnership. |
| 2 Support the sector's needs for open access, public confidence, and economic vitality while cost-effectively reducing physical and cyber risks and enhancing overall security and resilience. | PRIORITY C | Expand upon sector products, training, and exercises to enable owners and operators to reduce risk and improve readiness. |
| | PRIORITY D | Improve CF cybersecurity knowledge, tools, capabilities, risk assessments, and practices to secure critical cyber and physical assets linked to cyber systems. |
| 3 Increase capabilities and maintain advanced planning systems to ensure timely and effective response and recovery of critical services. | PRIORITY E | Enhance coordination with interdependent sectors and community response partners to improve resilience and enhance decision-making. |
| 4 Assess and analyze threats, vulnerabilities, and consequences to inform facility and sector-wide risk management. | PRIORITY F | Continue to conduct cyber and physical risk assessments and develop risk reduction strategies for evolving threats in collaboration with cross-sector, Federal, regional, and local security stakeholders. |
| 5 Promote continuous learning and adaptation during exercises, incidents, and planning. | PRIORITY G | Share security and resilience best practices and case studies to enable owners and operators to leverage lessons learned in all risk mitigation activities. |

## Value Proposition

The cooperation of owners and operators is essential to protect the CF Sector effectively and to ensure stakeholders receive the appropriate level of support for their security efforts. By participating in the CF Sector—through the CIPAC framework—owners and operators can:

- Express information-sharing needs to promote timely and accurate information sharing between the Federal Government and private sectors.
- Contribute to the CF SSP and ensure private and public sectors understand the value of and risks affecting the CF Sector.
- Identify best practices and policy recommendations to improve protection throughout the sector.
- Influence future decisions at the SLTT level, when it comes to addressing threats to commercial facilities and making resource allocation decisions regarding the sector.

Owner and operator participation in the CF Sector is essential to sustain the CF Sector's security and national image.

# 4.1 Commercial Facilities Sector Activities

CF Sector partners collaboratively identified a set of 24 activities as essential to achieving the CF Sector's goals and priorities. The following list reflects voluntary partnership activities that the sector may pursue over the next one to four years. While the SSPs are updated every four years, the CF Sector partnership may update its activities more frequently to reflect evolving risks, changing resource allocations, and partnership progress.

The GCC and SCC will meet annually to prioritize and build on the SSP activities listed here. During this time, the councils will further develop a list of discrete, detailed tasks to pursue over the coming year, considering timing, available resources, and feasibility.

Table 2. Commercial Facilities Sector Activities Mapped to Sector Priorities

| Map to Priority | | Sector Activities |
|---|---|---|
| A B | 1 | Improve DHS coordination with other Federal, State, regional, and local agencies—including the Federal Protective Service and General Services Administration—and centralize government sources for CF owners and operators to access information from across all agencies, including fusion centers. |
| A B | 2 | Formalize the process across DHS to provide sector feedback on intelligence that should be delivered at the For Official Use Only level. Increase the number of clearances in each CF subsector. |
| A B | 3 | Promote coordination among 77 fusion centers to connect nationwide information, particularly for national and global corporations. Use the Real Estate Information Sharing and Analysis Center as a resource. |
| A B | 4 | Increase awareness of the sector partnership framework, available resources, and strategic value to better engage all subsectors and small-scale owners and operators and recruit new members. Engage unions, Chambers of Commerce, and the Small Business Administration in security awareness training activities. |
| A B | 5 | Continue to expand the Real Estate Information Sharing and Analysis Center to include the Entertainment and Media, Outdoor Events, Public Assembly, and Sports Leagues Subsectors, and strengthen information-sharing relationships with owners and operators. |
| B | 6 | Reevaluate and restructure the CF Sector to optimize organization and reflect relationships between subsectors. |
| A F | 7 | Continue to conduct outreach for existing risks assessment tools/resources and leverage them to conduct onsite risk assessments at high-priority facilities. |
| C D | 8 | Leverage cyber-assessment capabilities from DHS and other Federal agencies to conduct onsite assessments and share common vulnerabilities across subsector facilities. |

| Map to Priority | | Sector Activities |
|---|---|---|
| D | 9 | Evaluate potential cyber risks and encourage CF Sector members to use the National Institute for Standards and Technology Cybersecurity Framework. Formulate communities of subsector IT experts (connected to the Sector Coordinating Council) to address sector-specific cyber threats. |
| B C | 10 | Expand armed attacker training to help smaller companies prepare and to provide materials for owners and operators to address employee training gaps. |
| B C G | 11 | Develop surveillance curriculum for security directors and leaders within the Surveillance Awareness Working Group. |
| B C E G | 12 | Develop a Sector Coordinating Council playbook for government and industry coordination and communication protocols during disaster response and recovery. |
| C E F | 13 | Develop an inventory of all documents and guides in each subsector. |
| A C F G | 14 | Track after-action reports from previous events across critical sectors to completion. |
| C E F | 15 | Work with the lifeline sectors, particularly the Energy and Water sectors, to examine strategies to sustain CF Sector operations during an interruption of services, such as by holding joint exercises, creating cross-sector councils, identifying ideas to improve resiliency, or organizing other activities. |
| E F | 16 | Work with the Emergency Services Sector and local officials to develop and conduct outreach for low-cost, unified, and nationwide response efforts—such as crisis reentry credentialing to ensure access to restricted areas after a disaster. |
| B F | 17 | Facilitate collaboration among owners, management companies, and tenants—along with Federal, State, and local partners—to improve joint risk mitigation and response to armed attacker threats. |
| E F | 18 | Collaborate with the Financial Services Sector to create a joint resource for logging the accessibility of ATM and banking resources during disasters, leveraging the Financial Services Information Sharing and Analysis Center and the Real Estate Information Sharing and Analysis Center. |
| B G | 19 | Work with Outdoor Events Subsector partners to increase resilience of outdoor events. |
| F G | 20 | Identify regions most at risk from climate change, determine which factors place them at risk, and develop mitigation strategies for CF infrastructure. |
| F G | 21 | Work with government and private sector partners, including the Federal Aviation Administration, to evaluate the emerging risk of unmanned aircraft systems and develop response strategies. |
| F G | 22 | Improve the sector's ability to leverage and respond to social media to enhance security during incidents and steady-state operations. |
| B G | 23 | Encourage more CF partners to seek SAFETY Act designation or certification, where appropriate. |
| A C E | 24 | Build on the Resilience Measurement Index to establish a resilience "score card" that helps owners and operators in the CF Sector and lifeline sectors determine how resilience is being measured and managed, and assists government agencies with tracking their effectiveness in information sharing. |

# 5 MEASURING EFFECTIVENESS

Owners and operators use a variety of indicators to measure the effectiveness and continuous improvement of their security and resilience measures and risk management processes at the facility level. Measuring improvements in security and resilience at the sector level is far more difficult. Where possible, the CF Sector attempts to measure how its voluntary partnership activities contribute to risk reduction and enhanced resilience across the sector.

As the SSA, DHS has the primary responsibility for measuring and reporting progress toward SSP activities using relevant metrics. An established performance metrics system designed to track the progress of sector activities is used to ensure accurate and consistent measurement.

The following table aligns CF Sector activities with a set of possible performance metrics that the SSA may use to measure and report progress, where possible. The metrics not only measure the completion of an activity—using output measures such as the number of products developed or partners engaged—but also aim to measure the *outcomes* of these activities—particularly how effective they are in achieving progress toward sector goals.

Within the voluntary sector partnership, often the best available outcome measure is to track the partners' intent to act based on the information, tools, or guidance they receive through sector activities. The SSA measures this intent to act using a survey of sector partners—during or following each engagement or activity—that asks them to indicate three things:

- Was the information received current and relevant?
- Will the information inform decision-making?
- Will participants further share the information within their organization?

Survey results indicate the effectiveness of each activity in equipping participants with the information, tools, guidance, and processes to take actions that ultimately reduce or better manage sector risk.

The SSA will report sector progress through the National Annual Report and the quadrennial SSP updates. The following list is not exhaustive of all possible ways to measure effectiveness, and sector asset owners may voluntarily measure and report additional information on sector progress during the National Annual Reporting process.

Table 3. Commercial Facilities Sector Activities and Expected Metrics

| | Commercial Facilities Sector Activities | Expected Metrics |
|---|---|---|
| **1** | Improve DHS coordination with other Federal, State, regional, and local agencies—including the Federal Protective Service and General Services Administration—and centralize government sources for CF owners and operators to access information from across all agencies, including fusion centers. | • Meetings and workshops organized or coordinated by the sector to simplify and synchronize coordination and information sharing<br>• Relevancy and intended use of information participants receive |
| **2** | Formalize the process across DHS to provide sector feedback on intelligence that should be delivered at the For Official Use Only level. Increase the number of clearances in each CF subsector. | • Meetings and workshops organized or coordinated by the sector to develop feedback process<br>• Number of clearance applications and clearances granted<br>• Relevancy and intended use of information participants receive |

| | Commercial Facilities Sector Activities | Expected Metrics |
|---|---|---|
| **3** | Promote coordination among 77 fusion centers to connect nationwide information, particularly for national and global corporations. Use the Real Estate Information Sharing and Analysis Center as a resource. | • Products developed from coordination efforts<br>• Relevancy and intended use of information participants receive |
| **4** | Increase awareness of the sector partnership framework, available resources, and strategic value to better engage all subsectors and small-scale owners and operators and to recruit new members. Engage unions, Chambers of Commerce, and the Small Business Administration in security awareness training activities. | • Meetings and workshops organized or coordinated by the sector to raise awareness<br>• Products developed and level of distribution<br>• Training activities organized or coordinated by the sector<br>• Relevancy and intended use of information participants receive |
| **5** | Continue to expand the Real Estate Information Sharing and Analysis Center to include the Entertainment and Media, Outdoor Events, Public Assembly, and Sports Leagues Subsectors, and strengthen information-sharing relationships with owners and operators. | • Status of expanding the RE-ISAC<br>• Relevancy and intended use of information participants receive from the RE-ISAC |
| **6** | Reevaluate and restructure the CF Sector to optimize organization and reflect relationships between subsectors. | • Meetings and working groups organized or coordinated by the sector<br>• Status of restructuring |
| **7** | Continue to conduct outreach for existing risks assessment tools/resources and leverage them to conduct onsite risk assessments at high-priority facilities. | • Meetings and workshops organized or coordinated by the sector as part of its outreach<br>• Products developed and level of distribution<br>• Relevancy and intended use of information participants receive |
| **8** | Leverage cyber-assessment capabilities from DHS and other Federal agencies to conduct onsite assessments and share common vulnerabilities across subsector facilities. | • Meetings or working groups organized or coordinated to share common vulnerability threads across subsector facilities<br>• Products developed to share common vulnerability threads<br>• Relevancy and intended use of information participants receive |
| **9** | Evaluate potential cyber risks and encourage CF Sector members to use the National Institute for Standards and Technology Cybersecurity Framework. Formulate communities of subsector IT experts (connected to the Sector Coordinating Council) to address sector-specific cyber threats. | • Meetings and working groups organized or coordinated to identify cyber risks or promote the NIST Cybersecurity Framework<br>• Status of establishing communities of IT experts<br>• Relevancy and intended use of information participants receive |
| **10** | Expand armed attacker training to help smaller companies prepare and to provide materials for owners and operators to address employee training gaps. | • Trainings developed and their level of participation<br>• Relevancy and intended use of information participants receive |

| | Commercial Facilities Sector Activities | Expected Metrics |
|---|---|---|
| **11** | Develop surveillance curriculum for security directors and leaders within the Surveillance Awareness Working Group. | • Status of developing curriculum<br>• Relevancy and intended use of information participants receive through the curriculum |
| **12** | Develop a Sector Coordinating Council playbook for government and industry coordination and communication protocols during disaster response and recovery. | • Status of developing an SCC playbook |
| **13** | Develop an inventory of all documents and guides in each subsector. | • Status of developing inventory<br>• How participants intend to use the information provided |
| **14** | Track after-action reports from previous events across critical sectors to completion. | • Status of developing an After-Action Report tracking system<br>• Products developed and level of distribution<br>• Relevancy and intended use of information participants receive |
| **15** | Work with the lifeline sectors, particularly the Energy and Water sectors, to examine strategies to sustain CF Sector operations during an interruption of services, such as by holding joint exercises, creating cross-sector councils, identifying ideas to improve resiliency, or organizing other activities. | • Joint exercises organized or coordinated and their level of participation<br>• Status of establishing cross-sector councils<br>• Meetings and working groups organized or coordinated to identify ideas to improve resilience<br>• Relevancy and intended use of information participants receive |
| **16** | Work with the Emergency Services Sector and local officials to develop and conduct outreach for low-cost, unified, and nationwide response efforts—such as crisis reentry credentialing to ensure access to restricted areas after a disaster. | • Meetings and working groups organized or coordinated to develop unified methods<br>• Status of establishing a credentialing program<br>• Products developed and their distribution<br>• Relevancy and intended use of information participants receive |
| **17** | Facilitate collaboration among owners, management companies, and tenants—along with Federal, State, and local partners—to improve joint risk mitigation and response to armed attacker threats. | • Meetings and working groups organized or coordinated<br>• Products developed<br>• How participants or recipients intend to use the information provided |
| **18** | Collaborate with the Financial Services Sector to create a joint resource for logging the accessibility of ATM and banking resources during disasters, leveraging the Financial Services Information Sharing and Analysis Center and the Real Estate Information Sharing and Analysis Center. | • Meetings and working groups organized or coordinated<br>• Products developed and level of distribution<br>• Relevancy and intended use of information participants receive |

| | Commercial Facilities Sector Activities | Expected Metrics |
|---|---|---|
| **19** | Work with Outdoor Events Subsector partners to increase resilience of outdoor events. | • Meetings and working groups organized or coordinated to identify opportunities to increase outdoor event management resilience<br>• Products developed and level of distribution<br>• Relevancy and intended use of information participants receive |
| **20** | Identify regions most at risk from climate change, determine which factors place them at risk, and develop mitigation strategies for CF infrastructure. | • Meetings and workshops organized or coordinated by the sector to identify regions most at risk from climate change impacts<br>• Products developed to mitigate climate change impacts in the identified regions<br>• Relevancy and intended use of information participants receive |
| **21** | Work with government and private sector partners, including the Federal Aviation Administration, to evaluate the emerging risk of unmanned aircraft systems and develop response strategies. | • Meetings and workshops organized or coordinated by the sector with partners to evaluate UAS risks and develop response strategies<br>• Products developed and level of distribution<br>• Relevancy and intended use of information participants receive |
| **22** | Improve the sector's ability to leverage and respond to social media to enhance security during incidents and steady-state operations. | • Products developed to address this need and level of distribution<br>• Meetings, workshops, or trainings organized or coordinated by the sector to improve the sector's social media capabilities<br>• Relevancy and intended use of information participants receive |
| **23** | Encourage more CF partners to seek SAFETY Act designation or certification, where appropriate. | • Meetings coordinated or organized to promote SAFETY Act designation/certification and the level of participation<br>• Products developed and level of distribution<br>• Relevancy and intended use of information participants receive |
| **24** | Build on the Resilience Measurement Index to establish a resilience "score card" that helps owners and operators in the CF Sector and lifeline sectors determine how resilience is being measured and managed, and assists government agencies with tracking their effectiveness in information sharing. | • Status of establishing a resilience "score card"<br>• Products developed and level of distribution<br>• Relevancy and intended use of information participants receive |

# APPENDIX A
## Acronyms and Terms

| | |
|---|---|
| **AARs** | after-action reports |
| **ADA** | Americans with Disabilities Act |
| **BCP** | Business Continuity Planning |
| **C³** | Critical Infrastructure Cyber Community Voluntary Program |
| **CBAT** | Computer-Based Assessment Tool |
| **CBR** | chemical/biological/radiological |
| **CBRE** | chemical/biological/radiological/explosive |
| **CDII** | Cyber-Dependent Infrastructure Identification |
| **CF** | Commercial Facilities |
| **CIPAC** | Critical Infrastructure Partnership Advisory Council |
| **CISR R&D** | *2015 National Critical Infrastructure Security and Resilience Research and Development Plan* |
| **CRR** | Cyber Resilience Review |
| **CS&C** | Office of Cybersecurity and Communications |
| **CSET** | Cybersecurity Evaluation Tool |
| **DHS** | U.S. Department of Homeland Security |
| **DOJ** | U.S. Department of Justice |
| **ECIP** | Enhanced Critical Infrastructure Protection |
| **EO** | Executive Order |
| **ESF** | Emergency Support Function |
| **FAA** | Federal Aviation Administration |
| **FBI** | Federal Bureau of Investigation |
| **FDA** | Food and Drug Administration |
| **FEMA** | Federal Emergency Management Agency |
| **FOUO** | For Official Use Only |
| **GCC** | Government Coordinating Council |
| **GDP** | gross domestic product |
| **GSA** | General Services Administration |
| **HSIN** | Homeland Security Information Network |
| **HSIN-CI** | Homeland Security Information Network – Critical Infrastructure |
| **HVAC** | heating, ventilation, and air conditioning |
| **HVEs** | homegrown violent extremists |
| **I&A** | Office of Intelligence & Analysis |
| **ICS** | Incident Command System |
| **ICS-CERT** | Industrial Control Systems Cyber Emergency Response Team |
| **IED** | improvised explosive device |
| **IP** | Office of Infrastructure Protection |
| **ISIL** | Islamic State of Iraq and the Levant |
| **IST** | Infrastructure Survey Tool |
| **IT** | Information Technology |
| **NFPA** | National Fire Protection Association |
| **NIPP 2013** | *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* |
| **NIST** | National Institute of Standards and Technology |
| **NSSE** | National Special Security Event |
| **OBP** | Office of Bombing Prevention |
| **OSHA** | Occupational Safety and Health Administration |
| **PPD** | Presidential Policy Directive |
| **PSA** | Protective Security Advisor |
| **R&D** | research & development |
| **RE-ISAC** | Real Estate Information Sharing and Analysis Center |
| **RMI** | Resilience Measurement Index |
| **RSF** | Recovery Support Function |
| **SAFETY Act** | Support Anti-terrorism by Fostering Effective Technologies Act |
| **SCC** | Sector Coordinating Council |
| **SEAR** | Special Event Activity Rating |
| **SLTT** | State, local, tribal, and territorial |
| **SLTTGCC** | State, Local, Tribal, and Territorial Government Coordinating Council |
| **SMEs** | subject matter experts |
| **SOPD** | Sector Outreach and Programs Division |
| **SSA** | Sector-Specific Agency |
| **SSP** | Sector-Specific Plan |
| **SSTEP** | Sector-Specific Tabletop Exercise Program |
| **U//FOUO** | Unclassified/For Official Use Only |
| **UAS** | unmanned aircraft systems |
| **USDA** | U.S. Department of Agriculture |
| **US-CERT** | United States Computer Emergency Readiness Team |

# APPENDIX B
## Alignment with the NIPP 2013

Table B-1. CF Sector Priorities Aligned with Joint National Priorities and NIPP Goals

| Commercial Facilities Sector Priorities | | Joint National Priorities | | | | | NIPP Goals |
|---|---|---|---|---|---|---|---|
| | | Strengthen Management of Cyber and Physical Risks to Critical Infrastructure | Build Capabilities and Coordination for Enhanced Incident Response and Recovery | Strengthen Collaboration Across Sectors, Jurisdictions, and Disciplines | Enhance Effectiveness in Resilience Decision-making | Share Information to Improve Prevention, Protection, Mitigation, Response, and Recovery Activities | |
| **A** | Improve formal public-private information sharing | | PRIORITY A | PRIORITY A | | PRIORITY A | Share information across the critical infrastructure community to build awareness and enable risk-informed decision-making. |
| **B** | Better encourage subsectors | | PRIORITY B | PRIORITY B | | PRIORITY B | |
| **C** | Expand sector products | PRIORITY C | | | PRIORITY C | | Secure critical infrastructure against physical, cyber, and human threats through sustainable risk reduction efforts, while considering costs and benefits. |
| **D** | Improve cybersecurity knowledge | PRIORITY D | PRIORITY D | PRIORITY D | PRIORITY D | | |
| **E** | Enhance coordination to improve resilience and decision-making | | PRIORITY E | PRIORITY E | PRIORITY E | PRIORITY E | Enhance critical infrastructure resilience by minimizing consequences and employing effective response and recovery. |
| **F** | Conduct risk assessments | PRIORITY F | | PRIORITY F | PRIORITY F | PRIORITY F | Assess and analyze risks to critical infrastructure to inform risk management activities. |
| **G** | Share security and resilience best practices | PRIORITY G | PRIORITY G | PRIORITY G | | PRIORITY G | Promote learning and adaptation during and after incidents and exercises. |

Table B-2. Contribution of the CF Sector Activities to the NIPP 2013 Calls to Action

| | Commercial Facility Sector Contribution or Aligned Activity | NIPP 2013 Calls to Action | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | #1 | #2 | #3 | #4 | #5 | #6 | #7 | #8 | #9 | #10 | #11 | #12 |
| 1 | Improve DHS coordination with other Federal, State, regional, and local agencies—including the Federal Protective Service and General Services Administration—and centralize government sources for CF owners and operators to access information from across all agencies, including fusion centers. | | | X | | | | X | X | | | | |
| 2 | Formalize the process across DHS to provide sector feedback on intelligence that should be delivered at the For Official Use Only level. Increase the number of clearances in each CF subsector. | | | | | X | | X | | | | | |
| 3 | Promote coordination among 77 fusion centers to connect nationwide information, particularly for national and global corporations. Use the Real Estate Information Sharing and Analysis Center as a resource. | | | | | X | | | | | | | |
| 4 | Increase awareness of the sector partnership framework, available resources, and strategic value to better engage all subsectors and small-scale owners and operators and to recruit new members. Engage unions, Chambers of Commerce, and the Small Business Administration in security awareness training activities. | | | X | | | | | | X | | | |
| 5 | Continue to expand the Real Estate Information Sharing and Analysis Center to include the Entertainment and Media, Outdoor Events, Public Assembly, and Sports Leagues Subsectors, and strengthen information-sharing relationships with owners and operators. | | | | | X | | | | | | | |
| 6 | Reevaluate and restructure the CF Sector to optimize organization and reflect relationships between subsectors. | | | | | | | | | X | | | |
| 7 | Continue to conduct outreach for existing risks assessment tools/resources and leverage them to conduct onsite risk assessments at high-priority facilities. | | | | X | | | | | | | | |
| 8 | Leverage cyber-assessment capabilities from DHS and other Federal agencies to conduct onsite assessments and share common vulnerabilities across subsector facilities. | | | | | X | | | | | | | |
| 9 | Evaluate potential cyber risks and encourage CF Sector members to use the National Institute for Standards and Technology Cybersecurity Framework. Formulate communities of subsector information technology experts (connected to the Sector Coordinating Council) to address sector-specific cyber threats. | | | | | X | | | | | | | |
| 10 | Expand armed attacker training to help smaller companies prepare and to provide materials for owners and operators to address employee training gaps. | | | | X | | | | | X | | | |
| 11 | Develop surveillance curriculum for security directors and leaders within the Surveillance Awareness Working Group. | | | | X | X | | | | X | | | |
| 12 | Develop a Sector Coordinating Council playbook for government and industry coordination and communication protocols during disaster response and recovery. | | | | | X | X | | | | | | X |
| 13 | Develop an inventory of all documents and guides in each subsector. | | | | | X | | | | X | | | |
| 14 | Track after-action reports from previous events across critical sectors to completion. | | | | | X | | | | | | | |
| 15 | Work with the lifeline sectors, particularly the Energy and Water sectors, to examine strategies to sustain CF Sector operations during an interruption of services, such as by holding joint exercises, creating cross-sector councils, identifying ideas to improve resiliency, or organizing other activities. | | | X | | X | X | | X | | | | X |
| 16 | Work with the Emergency Services Sector and local officials to develop and conduct outreach for low-cost, unified, and nationwide response efforts—such as crisis reentry credentialing to ensure access to restricted areas after a disaster. | | | X | | X | X | | X | | | | X |

| | Commercial Facility Sector Contribution or Aligned Activity | NIPP 2013 Calls to Action | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | #1 | #2 | #3 | #4 | #5 | #6 | #7 | #8 | #9 | #10 | #11 | #12 |
| 17 | Facilitate collaboration among owners, management companies, and tenants—along with Federal, State, and local partners—to improve joint risk mitigation and response to armed attacker threats. | | | | | X | | | | | | | |
| 18 | Collaborate with the Financial Services Sector to create a joint resource for logging the accessibility of ATM and banking resources during disasters, leveraging the Financial Services Information Sharing and Analysis Center and the Real Estate Information Sharing and Analysis Center. | | X | | | X | X | | X | | | | |
| 19 | Work with Outdoor Events Subsector partners to increase resilience of outdoor events. | | X | | | X | X | | X | | | | |
| 20 | Identify regions most at risk from climate change, determine which factors place them at risk, and develop mitigation strategies for CF infrastructure. | | | | X | X | | | | | | | |
| 21 | Work with government and private sector partners, including the Federal Aviation Administration, to evaluate the emerging risk of unmanned aircraft system use and develop response strategies. | | | | X | | | | | | | | |
| 22 | Improve the sector's ability to leverage and respond to social media to enhance security during incidents and steady-state operations. | | | | X | | | | | | | | |
| 23 | Encourage more CF partners to seek SAFETY Act designation or certification, where appropriate. | | | | X | | | | | | | | |
| 24 | Build on the Resilience Measurement Index to establish a resilience "score card" that helps owners and operators in the CF Sector and lifeline sectors determine how resilience is being measured and managed, and assists government agencies with tracking their effectiveness in information sharing. | | X | | X | | X | | | | | X | |
| | CF Sector goals and priorities were developed in alignment with the 2014 Joint National Priorities in support of Call to Action #1. | X | | | | | | | | | | | |
| | Development of the 2015 CF Sector-Specific Plan meets Call to Action #2. | | X | | | | | | | | | | |
| | The CF Sector supports Call to Action #10 by working with its Federal partners to implement the *National Critical Infrastructure Security and Resilience Research and Development Plan.* | | | | | | | | | | X | | |
| | The measurement approach outlined in Chapter 5: Measuring Effectiveness will enable the CF Sector to evaluate and report on the progress of partnership efforts, in support of Call to Action #11. | | | | | | | | | | | X | |

## NIPP 2013 Calls to Action

Call to Action #1: Set National Focus through Jointly Developed Priorities
Call to Action #2: Determine Collective Actions through Joint Planning Efforts
Call to Action #3: Empower Local and Regional Partnerships to Build Capacity Nationally
Call to Action #4: Leverage Incentives to Advance Security and Resilience
Call to Action #5: Enable Risk-Informed Decision-making through Enhanced Situational Awareness
Call to Action #6: Analyze Infrastructure Dependencies, Interdependencies, and Associated Cascading Effects
Call to Action #7: Identify, Assess, and Respond to Unanticipated Infrastructure Cascading Effects During and Following Incidents
Call to Action #8: Promote Infrastructure, Community, and Regional Recovery Following Incidents
Call to Action #9: Strengthen Coordinated Development and Delivery of Technical Assistance, Training, and Education
Call to Action #10: Improve Critical Infrastructure Security and Resilience by Advancing Research and Development Solutions
Call to Action #11: Evaluate Progress Toward the Achievement of Goals
Call to Action #12: Learn and Adapt During and After Exercises and Incidents

# APPENDIX C
# Commercial Facilities Sector Resources

## Exercises

### Sector-Specific Tabletop Exercise Program (SSTEP) for the Commercial Facilities Sector

The SSTEP allows users to leverage pre-built exercise templates and tailor them to their communities' specific needs in order to assess, develop, and update plans, programs, policies, and procedures within an incident management functional area. The SSTEP is an all-hazards risk management tool designed for critical infrastructure owners and operators focused on information sharing and coordination between sector-specific entities, the facility or venue, first responders, and other relevant stakeholders. The SSTEP materials provide a model exercise and support documentation that can be refined and further developed to exercise and evaluate specific areas of concern. The ability for public and private sector organizations to plan and execute SSTEP-based exercises will continue to enhance security and resilience by enabling these organizations to identify strengths and areas for improvement within their operating plans, techniques, and procedures. These identified issues are then developed into an improvement plan that clearly outlines the measures necessary to improve on current concepts. For more information, please contact the CF SSA at CFSTeam@hq.dhs.gov.

Completed CF SSTEPs available through Homeland Security Information Network – Critical Infrastructure (HSIN-CI) include:

- American Jewish Community
- Faith-Based Organizations
- Gaming
- Outdoor Events
- Retail
- Sports Leagues Facilities
- Workplace Violence

## Independent Study Courses

IS-100 Introduction to the Incident Command System (ICS)

IS-200 ICS for Single Resources and Initial Action Incidents

IS-700 National Incident Management System, An Introduction

IS-800 National Response Framework, An Introduction

IS-906 Workplace Security Awareness

IS-907 Active Shooter: What You Can Do

IS-909 Community Preparedness: Implementing Simple Activities for Everyone

IS-910 Emergency Management Preparedness Fundamentals

IS-912 Retail Security Awareness—Understanding the Hidden Hazards

IS-913 Critical Infrastructure Security and Resilience: Achieving Results through Partnership and Collaboration

IS-914 Surveillance Awareness: What You Can Do

IS-915 Protecting Critical Infrastructure Against Insider Threats

IS-916 Critical Infrastructure Security: Theft and Diversion—What You Can Do

# Publications

## *Active Shooter—How To Respond* Awareness Materials

The U.S. Department of Homeland Security (DHS) has developed a series of materials to assist businesses, government offices, and schools in preparing for and responding to an active shooter. These products include a desk reference guide, a reference poster, and a pocket-size reference card. The resources can be found on the Active Shooter Preparedness Webpage. Issues covered in the armed attacker materials include the following:

- Profile of an active shooter;
- Responding to an active shooter or other workplace violence situation;
- Training for an active shooter situation and creating an emergency action plan; and
- Tips for recognizing signs of potential workplace violence.

Available Materials

- Active Shooter Booklet
- Active Shooter Pamphlet
- Active Shooter Poster
- Active Shooter Poster (Spanish)
- Active Shooter Pocket Card
- Active Shooter Pocket Card (Spanish)

## Bomb-Making Materials Awareness Program

DHS developed the Bomb-Making Materials Awareness Program to assist commercial retailers, commercial service providers, and chemical distributors and wholesalers with identifying suspicious purchases of materials often used in the illicit manufacture of homemade explosives or improvised explosive devices (IEDs). In addition, the materials also inform retailers about the actions they should take if they notice suspicious behavior. For more information, please contact the Office for Bombing Prevention (OBP) at OBP@hq.dhs.gov. Available materials include:

- Bomb Threat Stand-Off Card
- Suicide Bomber Awareness Card
- Vehicle-Borne IED Identification Guide: Parked Vehicles
- Bomb-Making Materials Awareness Program Suspicious Behavior Cards

## Evacuation Planning Guides for Stadiums and Major Events

These two guides, the *Evacuation Planning Guide for Stadiums* and the *Mass Evacuation Planning Guide for Major Events: NASCAR Pilot*, assist stadium owners and operators with preparing evacuation plans and helping to determine when and how to evacuate, shelter-in-place, or relocate stadium spectators and participants. The *Evacuation Planning Guide for Stadiums* includes a template that can be used to create a plan that will incorporate the unique policies and procedures of State and local governments, surrounding communities, and specific stadium characteristics.

- *Evacuation Planning Guide for Stadiums*
- *Mass Evacuation Planning Guide for Major Events: NASCAR Pilot*
- *Mass Evacuation Planning Guide Appendices*

## Protective Measures Guides

These guides assist owners and operators in planning and managing security at their facilities. They provide an overview of threat, vulnerability, and protective measures and offer suggestions for successful planning, organizing, coordinating, communicating, operating, and training activities that contribute to a safe environment for guests and employees. To obtain For Official Use Only (FOUO)-designated documents, go to the Commercial Facilities site on HSIN-CI or contact CFSTeam@hq.dhs.gov. Current guides include:

- *Protective Measures Guide for U.S. Sports Leagues (FOUO)*
- *Protective Measures Guide for the U.S. Lodging Industry (FOUO)*

- *Protective Measures Guide for Mountain Resorts (FOUO)*
- *Protective Measures Guide for Outdoor Venues (FOUO)*

### Pandemic Influenza Planning Materials

Public assembly venue owners and operators use these pandemic influenza planning documents to enhance pandemic operational response planning. These two guides provide key steps and activities for managers of public assembly venues to consider when operating their facilities during pandemic situations. These guides are used in connection with the worksheet, which displays the status of operational activities that venues should use to respond to the influenza's effect on venues and surrounding areas. A checklist outlines the various activities that should be considered by public assembly venues when developing a pandemic response plan.

- *Pandemic Influenza Preparedness, Response, and Recovery Guide*
- *Pandemic Influenza Operational Review Worksheet*
- *Business Pandemic Planning Checklist*

### Hotel Security Poster: DHS Hotel and Lodging Advisory Poster

The DHS private sector advisory poster provides hotel employees with an increased awareness of their property's potential to be used for illicit purposes, suspicious behavior and items, and the appropriate actions to take if they notice suspicious activity. This "back-of-the-house" poster is available in both English and Spanish. To obtain copies of the DHS Hotel & Lodging Advisory poster, please contact the CF SSA at CFSTeam@hq.dhs.gov.

### Retail and Shopping Center Advisory Poster

This awareness poster helps train retail employees on the recognition of suspicious behavior that could indicate bomb-making activities, provides specific details on what may be considered suspicious, and encourages reporting of suspicious behavior. For more information, please contact the CF SSA at CFSTeam@hq.dhs.gov.

### Unclassified/For Official Use Only (U//FOUO) Complex Operating Environment for First Responders During Emergency Responses—Shopping Malls

This first responder reference aid is intended to promote coordination among Federal and SLTT government authorities and private sector security officials in deterring, preventing, disrupting, and responding to terrorist attacks. The graphic depicts the complex operating environment associated with shopping malls and highlights some pre-operational indicators commonly associated with the attack planning cycle. The product is not derived from ongoing threat streams to the Homeland, but was precipitated by the Nairobi, Kenya, mall attack, and should be considered in the context of potential events, locations, weapons and tactics, and existing agreements or policies within responding agencies' areas of responsibility.

### (U//FOUO) Complex Operating Environment for First Responders During Emergency Response—Stadiums and Arenas

This first responder reference aid is intended to promote coordination among Federal and SLTT authorities and private sector security officials in deterring, preventing, disrupting, and responding to terrorist attacks. The graphic, which depicts the complex operating environment associated with sporting venues, is not derived from ongoing threat streams to the Homeland, and should be considered in the context of potential events, locations, weapons and tactics, and existing agreements or policies within responding agencies' areas of responsibility.

### (U//FOUO) Complex Operating Environment—Unmanned Aircraft Systems/Remote Controlled Model Aircraft at Stadiums and Mass Gatherings

This first responder reference aid is intended to promote coordination among Federal and SLTT government authorities and private sector security officials in deterring, preventing, disrupting, and responding to terrorist attacks. The graphic, which depicts the complex operating environment presented by Unmanned Aircraft Systems/Remote Controlled Model Aircraft at stadiums and mass gatherings, is not in response to a specific threat to the Homeland and does not represent any particular venue. The information in this graphic should be considered in the context of potential events, locations, weapons and tactics, and existing agreements or policies within responding agencies' areas of responsibility.

### Sports Venue Bag Search Procedures Guide

This guide provides suggestions for developing and implementing bag search procedures at sporting event venues hosting major sporting events. The purpose for establishing bag search procedures is to control items that are hand carried into the sports venue. The bag search procedures should be a part of the venue's overall security plan and should be tested and

evaluated as outlined in the security plan. The actual implementation of bag search procedures and level of search detail will depend upon the threat to the venue as determined by the venue's security manager. For more information, please contact the CF SSA at CFSTeam@hq.dhs.gov.

### Sports Venue Credentialing Guide

This guide provides suggestions for developing and implementing credentialing procedures at sporting event venues that host professional sporting events. The purpose for establishing a credentialing program is to control and restrict access to a sports venue, and to provide venue management with information on those who have access. Credentialing can also be used to control and restrict vehicle movement within a venue. For more information, please contact the CF SSA at CFSTeam@hq.dhs.gov.

## Tools

### Cybersecurity Evaluation Program and Cyber Resilience Review (CRR)

CRRs are no-cost, non-technical, and voluntary assessments for organizations to measure cybersecurity capabilities against ten domains: asset management, controls management, configuration and change management, vulnerability management, incident management, service continuity management, risk management, external dependency management, training and awareness, and situational awareness. To schedule a facilitated CRR or to request additional information, please email the Cybersecurity Evaluation Program at CSE@hq.dhs.gov. For more information, visit the CRR Webpage.

### The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Cybersecurity Evaluation Tool (CSET)

ICS-CERT works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts. The Cybersecurity Evaluation Tool (CSET) is a DHS product that assists organizations in protecting their key national cyber assets. It was developed under the direction of the ICS-CERT by cybersecurity experts. This tool provides users with a systematic and repeatable approach for assessing the security posture of their cyber systems and networks. It includes both high-level and detailed questions related to all industrial control and information technology (IT) systems.

- Download CSET.
- Download the CSET Fact Sheet.
- To request onsite assistance, please send an email to cset@hq.dhs.gov.

### Suspicious Activity Reporting Tool (See: HSIN-CI under Additional Resources)

## Training and Workshops

### Active Shooter Preparedness Workshops

Scenario-based workshops feature facilitated discussions to engage private sector professionals and law enforcement representatives from Federal, State, and local agencies to learn how to prepare for and respond to an active shooter situation. Through the course of the exercise, participants evaluate current response concepts, plans, and capabilities for coordinated responses to active shooter incidents. To learn more, please contact ASworkshop@hq.dhs.gov.

### Bombing Prevention Training

OBP offers training to State, local, and private sector partners to enhance awareness of terrorist threats to the Nation's critical infrastructure. Workshops and courses educate participants on strategies for detecting and mitigating these threats.

### Bomb Threat Management Workshop (OBP@hq.dhs.gov)

This workshop enhances participants' knowledge, skills, and abilities concerning IEDs. Outlines specific safeties associated with bomb threat management and IED awareness, incidents, and prevention.

### Computer-Based Assessment Tool (CBAT) (CFSTeam@hq.dhs.gov)

CBAT is used to enhance vulnerability assessments and to assist in creating preparedness products.

### Improvised Explosive Device Counterterrorism Workshop (OBP@hq.dhs.gov)

This workshop educates private sector security professionals about counterterrorism tactics and techniques through exposure to key elements of soft target awareness, surveillance detection, and IED recognition.

### Improvised Explosive Device Search Procedures Workshop (OBP@hq.dhs.gov)

This workshop increases IED awareness and educates participants on bombing prevention measures and planning protocols to detect IEDs by reviewing specific search techniques. This workshop builds knowledge of counter-IED principles and techniques among first responders and public/private sector security partners tasked with IED search and response protocols.

### Infrastructure Survey Tool (IST) (CFSTeam@hq.dhs.gov)

The IST is a facility vulnerability assessment. ISTs are conducted by PSAs who take the collected data and evaluate the facility to determine the weakest and most vulnerable areas.

### Protective Measures (OBP@hq.dhs.gov)

This course builds awareness and understanding of IED threats, terrorist planning cycles, and indicators of suspicious activity. Participants learn about facility vulnerability analysis, counter-IED protective measures, and strategies that can be used to mitigate risk and reduce vulnerabilities.

### Surveillance Detection Training for Law Enforcement and Security Professionals (OBP@hq.dhs.gov)

Teaches operators and security staff how protective measures can detect and deter potential threats and covers the fundamentals for detecting surveillance activity. Participants apply skills, such as vulnerability and red zone analysis, surveillance detection, and observation and reporting, during practical exercises. FEMA EMI IS-914, Surveillance Awareness, is a prerequisite for this course.

### Vehicle-Borne Improvised Explosive Device Detection Course (OBP@hq.dhs.gov)

Improves the participant's ability to successfully inspect for, detect, identify, and respond to a vehicle-borne IED. Instruction covers the vehicle-borne IED threat, explosive effects, IEDs, and vehicle inspections, enabling participants to detect, deter, and protect against the illicit use of explosives.

### Videos

- Check It!—Designed to raise the level of awareness for front line facility employees by highlighting the indicators of suspicious activity, this video provides information to help employees properly search bags in order to protect venues and patrons across the country.
- No Reservations: Suspicious Behavior in Hotels—Designed to raise the level of awareness for hotel employees by highlighting the indicators of suspicious activity, this video provides information to help employees identify and report suspicious activities and threats in a timely manner.
- Options for Consideration: Active Shooter Preparedness Video—This video demonstrates possible actions to take if confronted with an active shooter scenario. It also shows how to assist authorities once law enforcement enters the scene. You may also access the video on YouTube.
- What's in Store: Ordinary People/Extraordinary Events—Designed to raise awareness for retail employees by highlighting the indicators of suspicious activity, this video provides information on identifying and reporting suspicious activity and threats at shopping centers and retail establishments.

## Webinars

### Active Shooter Awareness Virtual Roundtable

This 90-minute Webinar can help the private and public sector understand the importance of developing an emergency response plan and the need to train employees on how to respond if confronted with an active shooter. The presentation describes the three types of active shooter—workplace/school, criminal, and ideological—and how their planning cycles and behaviors differ.

### Critical Infrastructure Learning Series

The Critical Infrastructure Learning Series allows the Department to provide information and online seminars on current and emerging critical infrastructure topics to critical infrastructure owners and operators, government entities, and other partners.

### Evolving Threat

*Evolving Threat: What You Can Do* is a Webinar that includes a synopsis of evolving threats, followed by a protective measures presentation that helps owners and operators better protect their facilities, employees, and communities. The session combines subject matter experts, video scenarios, and valuable information to enhance security efforts.

### Hotel Security

*Safeguarding Hotels from the Threat of Terrorism* was developed in collaboration with the American Hotel & Lodging Association and provides information on key terrorism topics with reference to actual events. The Webinar includes a high-level briefing on the threat climate for the hotel industry and specific protective measures focusing on observing and reporting suspicious activity and items. The Webinar focuses on terrorism topics including, but not limited to, lessons learned from Mumbai-style attacks, IED awareness and response, and active shooter scenarios.

### Improvised Explosive Device Threat Awareness and Detection

*Improvised Explosive Device Threat Awareness and Detection* focuses on IEDs. The training provides awareness-level information for staff, management, and security to recognize, report, and react to unusual activities and threats in a timely manner.

### Retail Security

- *Active Threat Recognition for Retail Security Officers* is an 85-minute presentation discussing signs of criminal and terrorist activity, types of surveillance, and suspicious behavioral indicators. To access a recording of this Webinar, please register. After submitting the registration information, you will receive an email confirmation with instructions for logging in to the view the material.
- *Threat Detection & Reaction for Retail & Shopping Center Staff* is a 20-minute presentation intended for point-of-sale staff, but is applicable to all employees of a shopping center, mall, or retail facility. It uses case studies and best practices to explain suspicious behavior and packages, how to reduce the vulnerability to an active shooter threat, and the appropriate actions to take if employees notice suspicious activity.
- *Cybersecurity in the Retail Sector* provides retail employees and managers with an overview of cyber threats and vulnerabilities facing the industry. The Webinar also reviews the types of cyber systems and infrastructure used by the retail industry and steps that retail personnel can take to address the unique vulnerabilities to those cyber resources.

### Shopping Centers Security Terrorism Awareness Training

The Shopping Center Security Terrorism Awareness Training Program provides security personnel with increased awareness of the various facets of terrorism and criminal activity that could occur at a retail facility. During this course, participants will examine weapons that may be used in a terror attack and will be able to describe various attack tactics that may be used against a retail facility. Participants will also be able to assess potentially suspicious behavior and will be able to conduct surveillance at their facility. The course also describes proper response to terrorist or criminal incidents. To access the presentation, please register.

### Surveillance Detection

*Surveillance Detection Awareness on the Job* is part of the "If You See Something, Say Something™" campaign to raise public awareness of potential indicators of terrorism, crime, and other threats, and to emphasize the importance of reporting suspicious activity to law enforcement authorities. This free, online interactive session of video scenarios, commentary by a panel of experts, and questions and comments will better prepare participants to guard against surveillance activities.

## Additional Resources

### Homeland Security Information Network (HSIN)

- HSIN is an Internet-based platform used by DHS to facilitate information sharing necessary for coordination, operational plans, mitigation, and response to incidents by the government and the private sector. HSIN allows for secure, encrypted communications between DHS and the private sector, including sector-specific threat information. The CF Sector maintains an independent site on the HSIN portal.
- Suspicious activity can be reported on the HSIN Suspicious Activity Reporting Tool. The tool is meant to supplement, not replace, other means of suspicious activity reporting and is a standardized means by which critical infrastructure partners can report suspicious or unusual activities to the government via sector sites on the HSIN-CI.

### Business Continuity Planning Suite

The Business Continuity Planning (BCP) Suite was developed to assist businesses across all sectors with the need to create, improve, or update their business continuity plans. The Suite was designed to be user-friendly and scalable for optimal organizational use. It consists of three main components that include BCP training, automated BCP and disaster recovery plan generators, and a self-directed exercise for testing an implemented BCP. Businesses can utilize this solution to maintain

normal operations and exhibit resilience during a disruptive event. For more information on the BCP Suite, contact criticalmanufacturing@hq.dhs.gov.

### Commercial Facilities Sector Webpage

The Commercial Facilities Sector Webpage includes links to various resources, trainings, and publications useful for sector partners."

### "If You See Something, Say Something™"

In July 2010, DHS, at Secretary Janet Napolitano's direction, launched a national "If You See Something, Say Something™" campaign—a simple and effective program to raise public awareness of indicators of terrorism and terrorism-related crime, and to emphasize the importance of reporting suspicious activity to the proper State and local law enforcement authorities.

### Protective Security Advisors (PSAs)

The PSA Program's overarching mission is to proactively engage with SLTT government mission partners and members of the private sector stakeholder community to protect the Nation's critical infrastructure. Regional Directors and PSAs are security subject matter experts that serve as the link between SLTT organizations and DHS infrastructure mission partners. By performing vulnerability and security assessments to identify security gaps and potential vulnerabilities as well as coordinating National Protection and Programs Directorate/Office of Infrastructure Protection (IP) training and supporting incident management, PSAs serve as a vital channel of communications for officials and private owners and operators of critical infrastructure assets seeking to communicate with DHS. Private sector owners and operators interested in contacting their PSA should contact the DHS Protective Security Coordination Division Operations Desk at pscdoperations@hq.dhs.gov or 703-235-9349. For more information, visit the PSA Program Webpage.

### Support Anti-terrorism by Fostering Effective Technologies Act (SAFETY Act)

The SAFETY Act provides important legal liability protections for providers of Qualified Anti-Terrorism Technologies—either products or services. The goal of the SAFETY Act is to encourage the development and deployment of new and innovative antiterrorism products and services by providing liability protections. For more information, visit the SAFETY Act Webpage.

### Retail Security Resources DVD

The Retail Security Resources DVD contains fact sheets, posters, and awareness cards for security professionals. DVD materials may also be found on HSIN. To request a copy, please contact the CF SSA at CFSTeam@hq.dhs.gov. The DVD contains:

- Are You Aware of Suspicious Activity? Poster (DHS/IP/SOPD)
- Hazardous Chemicals Poster (DHS/IP/OBP & FBI)
- Hazardous Chemical Awareness Card (DHS/IP/OBP & FBI)
- Office of Bomb Prevention Fact Sheet (DHS/IP/OBP)
- Peroxide Products Poster (DHS/IP/OBP & FBI)
- Peroxide Product Awareness Card (DHS/IP/OBP & FBI)
- Precursor Chemicals Poster for Online Retailers (DHS/IP/OBP & FBI)
- Suspicious Behavior Poster (DHS/IP/OBP & FBI)
- Suspicious Online Purchases (DHS/IP/OBP & FBI)
- TRIPwire Fact Sheet (DHS/IP/OBP)


Homeland
Security