VENUE GUIDE FOR MITIGATING DEPENDENCY DISRUPTIONS

DECEMBER 2025

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

CONTENTS

INTRODUCTION

The United States faces a dynamic threat environment that challenges the security and safety of critical infrastructure. This includes man-made threats and natural hazards that can significantly disrupt operations and impact many lives. Enhancing the protection and resilience of critical infrastructure is paramount to sustaining the American way of life. To achieve this goal, in addition to considering the immediate facility perimeter, owners and/or operators of public gathering venues that host events must also account for the services upon which the critical infrastructure depends. This is of particular importance for services associated with the lifeline sectors—Energy, Water and Wastewater Systems, Communications, and Transportation Systems.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has developed this guide to provide baseline considerations to help critical infrastructure owners and/or operators mitigate the consequences of potential disruptions to a public gathering venue's lifeline sectors. This guide is not all-encompassing and should be used in conjunction with other CISA documents, such as the Venue Guide for Security Enhancements, to support a comprehensive view of protection and resilience.

BACKGROUND AND CONTEXT

CISA leads efforts to protect the nation's cyber and physical infrastructure by providing clear guidelines and support for risk management, incident response, and infrastructure protection. CISA developed the *Venue Guide for Mitigating Dependency Disruptions* to equip public gathering venue owners and/or operators with effective strategies to safeguard operations, mitigate vulnerabilities, and enhance preparedness.

OVERVIEW OF THE RISK ENVIRONMENT

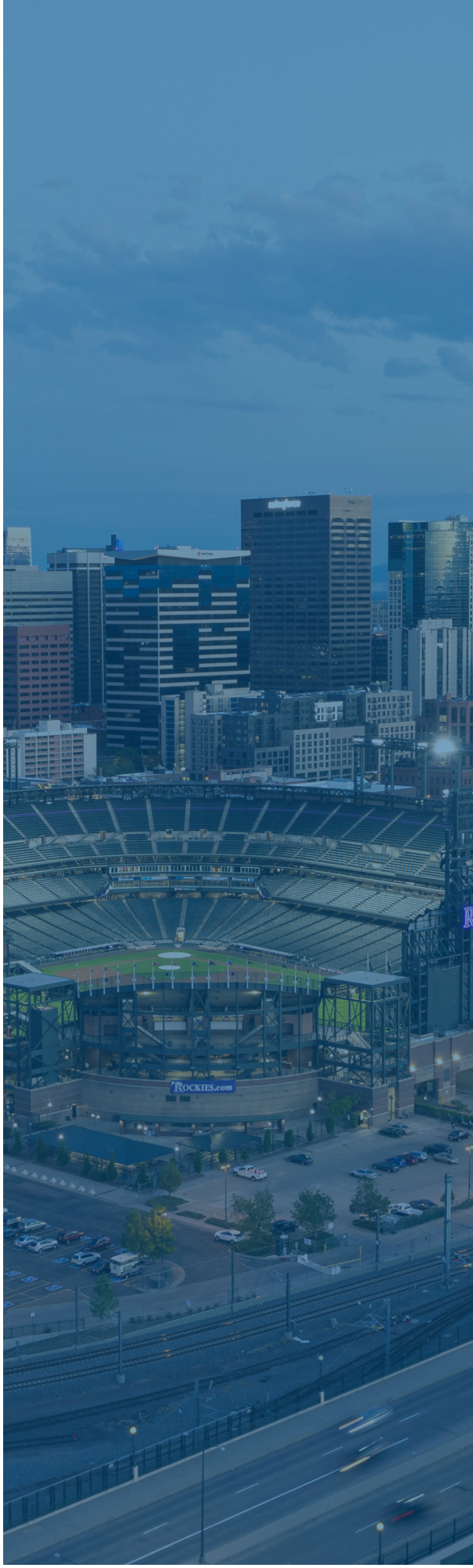
The 2025 Homeland Threat Assessment identifies nation-state cyber actors, domestic violence extremists, and foreign terrorist organizations as major threats to U.S. critical infrastructure and public gathering venues in the coming years. Public gathering venue owners and/or operators must manage a dynamic and evolving set of risks that pose significant challenges to venue security, event management, and public safety. The essential services provided by the lifeline sectors—Energy, Water and Wastewater Systems, Communications, and Transportation Systems—are a particularly important component of that risk. Public gathering venues must be able to identify vulnerabilities related to lifeline sectors and services, and determine appropriate responses or mitigation strategies in the event of a disruption.

UNDERSTANDING DEPENDENCIES AND LIFELINE SECTORS

Public gathering venue owners and/or operators rely on the lifeline sectors to deliver essential services. When the availability of a service is disrupted, public gathering venue staff and personnel must ensure a plan is in place to keep all staff and patrons safe, and to ensure the continued operation of the event.

The services provided by the lifeline sectors—Energy, Water and Wastewater Systems, Communications, and Transportation Systems—are critical to the operations of almost all other sectors, as well as each other, and are fundamental to the delivery of essential services related to immediate public health and safety. They are sometimes referred to as the critical services sectors, key sectors, lifeline interdependencies, or lifeline sectors. This document will henceforth refer to them as the **lifeline sectors.**

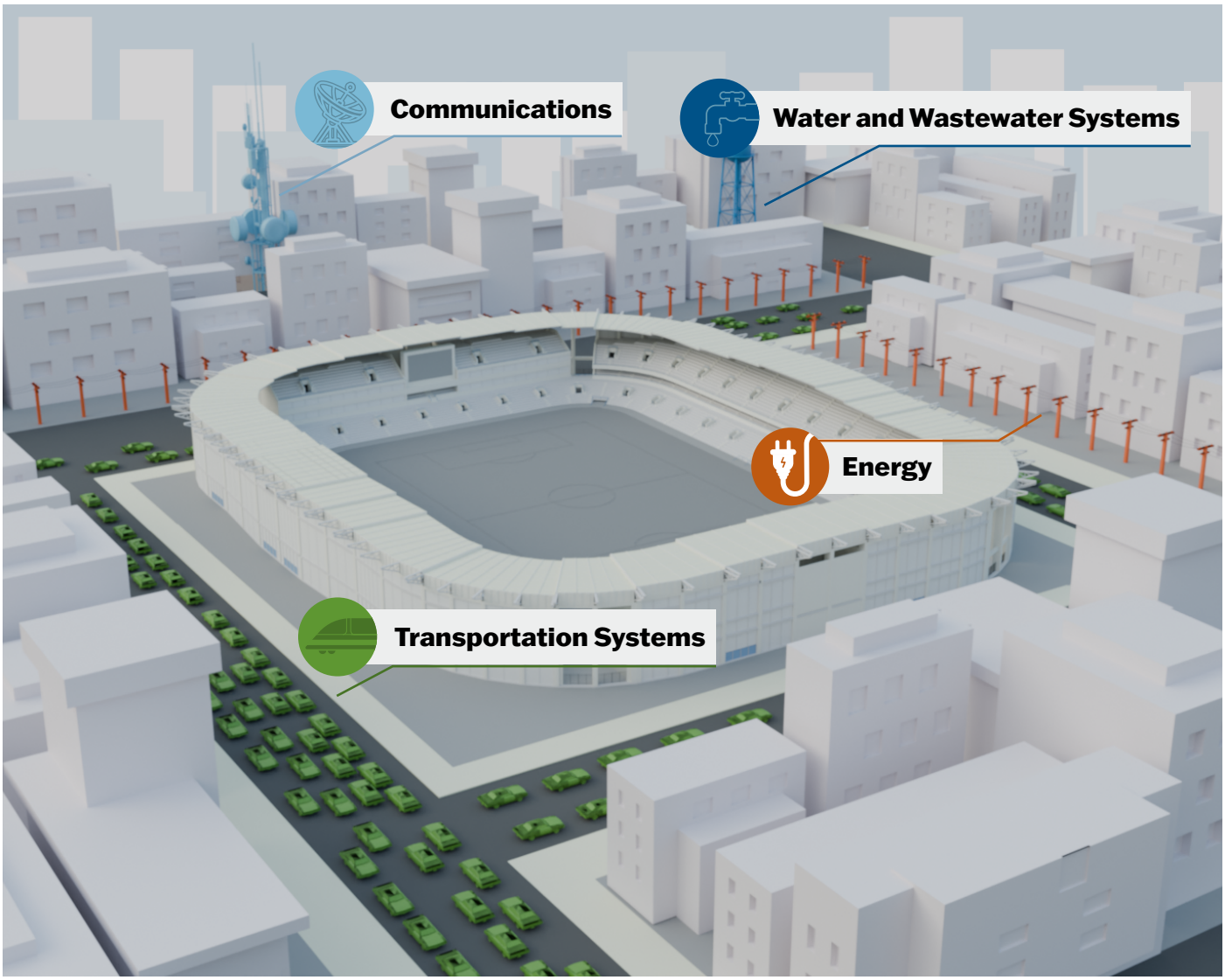
Dependencies are relationships of reliance within and among infrastructure systems and assets. They can be physical, geographic, cyber, or logical. Dependencies flow both ways, with multiple systems relying on each other simultaneously. A threat or hazard can result in the loss of a service, potentially affecting the critical infrastructure requiring this resource for operation. This can further impact other critical infrastructure dependent upon that system's services. The total consequences of an event are amplified by the dependencies and interdependencies that exist among critical infrastructure facilities and systems. **Interdependency** refers to a relationship where the consequences of a positive or an adverse event affecting one sector will have cascading effects upon others.



LIFELINE SECTORS AND VULNERABILITIES

A vulnerability is defined as a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. Because public gathering venues rely on the essential services and functions that the lifeline sectors provide, they are vulnerable to disruptions that impact the lifeline sectors.

Understanding how critical infrastructure systems and assets are interconnected via dependencies is essential to identifying and evaluating a public gathering venue's risks and vulnerabilities. Public gathering venue operators cannot evaluate every vulnerability. However, they can proactively identify the vulnerabilities that may be impacted by a dependent service through assessments, and their inclusion in contingency plans can reduce potential consequences.



The following sections examine each lifeline sector in closer detail by identifying the potential threats or hazards associated with that sector, potential consequences to a public gathering venue in the event of disruption, and security enhancements that public gathering venue owners and/or operators can implement to mitigate such incidents. Each sector is composed of multiple systems, with each point of intersection between them representing a dependency—and therefore a vulnerability.

ENERGY

Energy systems power every other critical infrastructure system and are critical to the delivery of essential services such as healthcare and media, and provide the underlying services that enable the economy. Fundamentally, energy systems keep the lights on, buildings warm, food cool, vehicles moving, and information flowing.

Consequences

- Loss of lighting throughout facility
- Game/event operational delays
- Heat/cold injuries
- Security system deficiencies
- Communications system deficiencies
- Food/drink vendor operational delays
- Broadcast/commercial revenue deficiencies
- Fire suppression deficiencies
- Crowd panic/crowd crush
- Loss of elevators, escalators, and/or other electrical mechanical egress and ingress capabilities

Security and Resilience Enhancements

- Establish redundancy for lighting, elevators, escalators, environmental heating/cooling, food and drink cooking/dispensing, communications and score boards, security and access systems, and water pumping.
- Consult with information technology/security officers to help identify the cyber infrastructure assets and systems related to the facility and to inform planning decisions.
- Seek multi-agency coordination with energy providers, municipal authorities, and neighboring businesses to plan contingencies.
- Establish a non-electric means of communication—such as visible banners, portable battery-powered audio and signage, or verbal message relay—for messaging with fans/attendees and facility staff.
- Establish a non-electric-dependent means of communication—such as radio and cellular phone connection—for communication with responders and external stakeholders.
- Conduct staff training to manage contingencies (e.g., immediately close elevator and escalator access, train to assist first responders to help those who are trapped).
- Acquire backup generators and a supply of fuel.
- Create an emergency contacts list for critical energy supplies.
- Acquire alternatives for backup power.
- Connect with local providers for scheduled "brownouts" and to ensure the facility is added to a preferred customer list. Energy providers will issue sufficient notification to run on backup power to avoid disruptions.
- Connect with secondary providers.
- Develop a Continuity of Operations Plan (COOP).
- Test and schedule maintenance for all backup power systems.
- Prioritize asset response actions in the event of an energy disruption.
- Establish agreements for the provision of and payment for onsite standby repair staff.
- Ensure physical security of onsite energy assets.

Potential Threats/Hazards to Energy Systems

- Disruptive physical or cyberattacks on electrical infrastructure
- Physical attack on infrastructure or substations
- Weather or solar storm impact to electric grid
- Equipment failure
- Local outage
- Brownouts
- Cyber or physical attack on individual energy assets
- Fire
- Electromagnetic Pulse (EMP)
- Human error
- Aging infrastructure

Key Stakeholders

- Local energy providers
- Energy generation representatives
- Federal, state, and local government stakeholders
- Neighboring businesses

CASE STUDY

FOOTBALL GAME

IMPACT

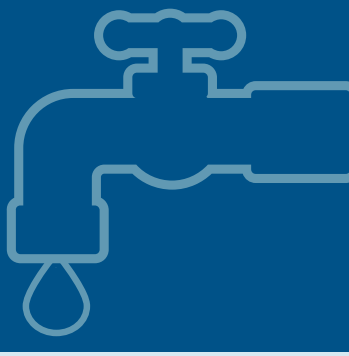
In 2013, an equipment failure within a large stadium led to a 34-minute power disruption during an internationally televised championship football game. The live broadcast of the game was suspended during the outage. The partial power outage was traced back to a "smart" electrical relay device housed less than a mile from the public gathering venue. The outage caused confusion and frustration among attendees, players, and personnel before power was fully restored.

RESOLUTION

In light of the power disruption in 2013, stadium operators added layers of security and took additional proactive measures prior to hosting a championship game in 2025, including the installation of LED lights and enhanced security at its power vault and substations. The city's local electric supplier replaced old equipment; two substations now power the facility, and three feeder lines connect the substations to the stadium vault.

WATER AND WASTEWATER SYSTEMS

Water infrastructure consists of both drinking water and wastewater systems, which are essential to the fulfillment of basic societal functions. Drinking water is required for sustaining life and protecting public health. Collection and treatment of wastewater is vital for preventing disease and protecting the environment.



Consequences

- Sanitation disruptions
- Loss of public lavatories
- Dehydration-related injuries
- Heating/cooling deficiencies
- Facility field and landscaping maintenance issues
- Inability to suppress fire
- Illness due to contamination
- Loss of power
- Injuries and possible death
- Underground water main breaks, which can severely damage roadway infrastructure, create sinkholes, and present challenges for both vehicles and pedestrians

Security and Resilience Enhancements

- Develop a COOP.
- Communicate regularly with water and wastewater service providers.
- Schedule regular inspections of water and wastewater systems at the facility.
- Develop a backup plan in place for drinking water for designated period of time.
- Ensure redundancies for sanitation, cooling, field and landscaping maintenance, and drinking water.
- Establish a routine, reliable water testing regimen with internal or external technicians to ensure the safety and potability of drinking water.
- Establish multi-agency coordination with water providers, municipal authorities, and neighboring businesses to plan contingencies.
- Retain contracts that can be quickly activated for the delivery of portable toilets/restroom trailers on site in the event of a sustained water outage.
- Maintain access to or a supply of bottled water for rapid distribution, particularly in very hot weather.
- Train and alert onsite first aid staff to prepare for treatment of a higher-than-usual number of dehydration and heat related illnesses.
- Maintain, by prior agreement, standby responder capability for surge capacity.
- Conduct exercises with stakeholders to test response, resilience, and COOPs.
- Establish agreements for the provision of and payment for onsite standby repair staff.

Potential Threats/Hazards to Dependency Systems


Cyberattack targeting water treatment plant or pump stations


Disruptive physical or cyberattacks on pipelines or water treatment plants


Insider Threats and Environmental Hazards (e.g., algal blooms, zebra mussels, waterborne diseases)


Equipment failure


Severe weather


Human error


Aging infrastructure

Key Stakeholders

- Local drinking water and wastewater service providers, including stormwater utilities
- Federal, state, and local government stakeholders
- Neighboring businesses

CASE STUDY

HOCKEY MATCH

IMPACT

In 2022, a water main break in downtown Nashville, Tennessee flooded the surrounding area, including local businesses and a hockey arena. Water flooded the arena's loading dock, locker rooms, and main event floor. As a result, the hockey team was forced to postpone two prime-time televised games. The flooding resulted in loss of income, insurance costs, and significant damage to the arena, as well as frustrated fans.

RESOLUTION

City and venue staff restored the arena in time for the third game of the season. According to arena staff, "millions of gallons" of water damaged the facility's ducts, electrical systems, communications boards, and TV room. A temporary TV room operated the scoreboard and game clock for the next several games due to the damage. Arena staff punched holes in several walls to facilitate drying, and almost all ceiling tiles and carpets were replaced. The arena was able to host a major concert four days later but incurred significant costs associated with the cleanup.

COMMUNICATIONS

Communications systems are critical to virtually every societal function a community provides, both big and small. Communications systems are needed to monitor, control, and manage nearly every aspect of infrastructure operations. Without them, everything from providing clean water to managing the flow of energy becomes much more difficult.

Consequences

- Loss of key security services
- Inability to communicate with venue attendees
- Operational game/concert day disruptions
- Crowd panic/crowd crush
- Inability to contact and coordinate with first responders
- Delayed crisis responses
- Sensitive information exposed to cybersecurity threats
- Delay in emergency services interdependent on inability to suppress fire or loss of power affecting communications
- Disruption of movement of money, especially with mobile payment applications and wireless sales points

Security and Resilience Enhancements

- Establish and exercise Primary, Alternate, Contingency, Emergency (PACE) communications plan to help prepare for critical communications in out-of-the-ordinary situations and establish options for redundant communications capabilities if primary capabilities are disrupted or degraded. For example, establish redundant fiber circuits and feeds with multiple providers to reduce impact of a single circuit failure.
- Maintain redundancies for cell phone access, business administrative services, emergency communications, and security and access systems.
- Ensure supply chain is secure from cyber threats.
- Ensure physical security to protect enterprise network.
- Isolate key systems to ensure they are not compromised in the event of an attack on the enterprise system.
- Screen third-party vendors for ongoing cyber hygiene.
- Ensure relevant staff are trained on security controls and shared risk components.
- Invest in redundant communications facilities, leverage routing contingency plans, and augment backup communications facilities to minimize service disruptions.
- Deploy spare parts to staging areas close to, but outside of, impact zones in advance of a weather event.
- Join and participate in Communications Information Sharing and Analysis Center (Comm-ISAC) sessions. Comm-ISAC is free to join.
- Ensure physical diversity for critical communications paths.
- Establish resilient supply chains leveraging multiple sources for critical parts.
- Support the infrastructure that feeds into the communications equipment and infrastructure at venue.

Potential Threats/Hazards to Dependency Systems

- Natural hazard impacting telecommunications systems
- Disruptive physical or cyberattacks on telecommunications
- Skilled workforce shortage
- Legacy or unauthorized components
- Human error
- Aging infrastructure

Key Stakeholders

- Telecommunications service providers and satellite service providers
- State and local law enforcement, public safety personnel, and emergency management
- Statewide Interoperability Coordinators (SWICs)
- Neighboring businesses

CASE STUDY

CONCERT BOMBING

IMPACT

In 2017, a suicide bombing attack at a music venue in England killed 22 people as they were leaving a concert. A communications failure occurred when family members of concertgoers attempted to call into the 0800 “casualty bureau” telephone number, a phone line set up for police to give key information to families. The phone number, however, was not activated in a timely manner. Due to external factors outside of the venue operator’s control, including high call volume, the casualty bureau service failed to operate as intended, causing distress, anxiety, and frustration among those at the venue and their family members.

RESOLUTION

Following extensive inquiry into the causes of and response to the devastating attack, the service provider for the incident line undertook a major upgrade to its capabilities. The provider also instituted daily testing of the system to ensure the issue was not repeated.

TRANSPORTATION SYSTEMS

Transportation systems support basic societal functions by facilitating the movement of people and everyday necessities. Without them, ambulances could not respond to emergencies and store shelves would be bare. Transportation infrastructure consists of three main systems: air systems, surface systems, and maritime systems.

Consequences

- Traffic congestion
- Patron frustration
- Delays in public transportation
- Overcrowding
- Panic and chaos
- Compromised public safety
- Disruption of emergency services
- Supply chain disruptions

Security and Resilience Enhancements

- Determine if the facility is adjacent to any major public transportation hubs.
- Determine how most attendees travel to facility.
- Conduct mission and asset specific risk assessments to identify potential risks, evaluating the likelihood and impact of a disruption, and implementing mitigating measures to ensure safety and efficiency.
- Develop contingency plans and protocols.
- Address infrastructure weaknesses.
- Implement redundant systems or backup components for critical assets for minimizing downtime and ensuring continuous availability of critical systems and services. (i.e., hardware, storage systems, N + 1 configuration, and failure strategies).
- Conduct training and exercises.
- Coordinate with key stakeholders.
- Deploy barriers to protect dedicated ride-share areas.
- Determine if public transportation modes run after-hours in the event the start of a performance or game has been delayed due to other circumstances.
- Negotiate and sign Memorandum of Understanding with contingency transportation providers (such as bus companies) to enable evacuation from an area in the event of a major public transportation mode outage.

Potential Threats/Hazards to Dependency Systems

- Power outages
- Human error
- Aging infrastructure
- Technological failures
- Disruptive physical or cyberattacks on transportation systems
- Rail sabotages
- Extreme weather events
- Threat to public safety

Key Stakeholders

- Public transit authorities/ providers
- State and county departments of transportation
- Regional transportation authorities/planners
- Neighboring businesses

CASE STUDY

SUMMER OLYMPICS

IMPACT

In 2024, on the day of the opening ceremony of the Olympics, arsonists attacked France's high-speed rail network, setting fires that paralyzed train travel to Paris for 800,000 people across Europe, including athletes heading to the opening ceremony.

RESOLUTION

Intelligence services and law enforcement were rapidly deployed to investigate and address the sabotage. Emergency measures were implemented to manage the transportation crisis, including rerouting trains and providing alternative travel options.

SECURITY RISK ASSESSMENTS AND ASSOCIATED KEY COMPONENTS

A comprehensive security risk assessment can identify potential vulnerabilities and support the identification of corresponding mitigating measures. The first step of a security risk assessment is to identify and prioritize the public gathering venue's assets in relation to the criticality of the organization's mission and determine the consequences that could occur if those assets were compromised.

Infrastructure vulnerabilities, such as unreliable power systems, weak cybersecurity, and irregular maintenance can create cascading failures. While specific risks vary by organization, security risk assessments help prioritize security improvements.

Risk Assessment

Identify and prioritize the public gathering venue's critical assets. Conduct pre-event assessment to identify threats, hazards, gaps, and security measures. Treat each event as unique with its own security requirements.

Mitigation

Select and implement security and other measures to address the identified and prioritized risks to the venue and event.

Information Sharing

Share intelligence and information about threats, suspicious behavior, and previous incidents with neighboring facilities and sectors

Local Collaboration

Partner with law enforcement, transportation, communications, energy, and water and wastewater management entities.

Area Awareness

Monitor local events like political rallies, celebrity appearances, markets, or fairs that may impact security.

Documentation

Maintain current emergency response, evacuation, and crowd control management protocols.

Training

Ensure comprehensive training for staff, volunteers, and vendors on policies and procedures.

Exercises

Implement tabletop or operational exercises to strengthen multi-agency coordination.

Resources

Utilize available resources through government agencies like CISA and professional associations.

CONTINUED PARTNERSHIPS

Partnerships and collaboration are essential for the protection of critical infrastructure across public and private sectors. Through these partnerships, two-way information sharing of threats, risk mitigation, and other vital information plays a significant role in mitigating potential disruptions to public gatherings. This mutual commitment to information sharing, combined unique resources, and competencies maximizes safety and security for public gathering venue owners and/or operators and event managers. The following partnerships and resources are available to support emergency response and contingency plan development:

CISA Security Advisors

Support organizations with critical infrastructure vulnerability assessments. CISA provides local physical security and cybersecurity experts who engage with all levels of government and the private sector to help protect critical infrastructure. CISA's Security Advisors provide technical assistance, support training requirements, conduct security surveys and assessments, and assist with security planning.

Organizational Planning Actions

Coordinate notification and response plans with partners through appropriate channels.

Localized Partnerships

Establish contact with local services providers and request to be added to the "preferred customer list." Service providers will support public gathering venues in the event of a disruption. Utilize CISA's Planning Participant Contact Information Worksheet to keep track of contact information for various service providers and other partners.

Stay notified of scheduled brownouts. A brownout is a temporary reduction in voltage that can cause dimming lights and reduced performance of devices. Some brownouts are scheduled intentionally by power providers to reduce overburdened systems. Brownouts are less disruptive than full outages but can still affect electrical equipment. Ensure that the public gathering venue is included in a "preferred customer list" to minimize disruptions to an event.

Maintain other localized partnerships. Establishing localized partnerships that foster trust and effective coordination is a key to maintaining critical infrastructure security and resilience. Localized partnerships include surrounding businesses, local emergency response teams, local food and beverage services, and markets. Through these partnerships, we facilitate a team environment where two-way information sharing of critical threat information, risk mitigation, and other vital information and resources is quick, seamless and actionable. This mutual commitment to information sharing through our trusted partnerships is essential to enhance security.

Critical Infrastructure Sector Partnerships

Information Sharing and Analysis Centers (ISACs): ISACs are membership-based, federally supported collaboratives that are open to state, local, tribal, and territorial entities. Members receive direct access to a suite of services and informational products including cybersecurity advisories and alerts, vulnerability assessments, incident response support, secure information sharing, tabletop exercises, a weekly malicious domains/IP report, and more.

KEY TERMS

Asset Criticality Analysis: The identification, categorization, and prioritization of critical assets in relation to the facility's mission, conducted at the beginning of a security risk assessment.

Consequence Analysis: The process of understanding, describing, and ranking the impacts of the loss of the facility's critical assets.

COOP (Continuity of Operations Plan): A predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations.

Dependency: A relationship of reliance within and among infrastructure assets and systems that must be maintained for those systems to operate and provide services. The National Infrastructure Protection Plan affirms that understanding critical infrastructure dependencies is essential to enhancing the resilience of communities.

Disruption: The interruption of an event, activity, or process. For the purposes of this guide, disruptions are defined as unexpected interruptions.

Hazard: A natural or human-caused source or cause of harm or difficulty. Unlike a threat, a hazard is not directed at a target.

Interdependency: A relationship where the consequences of a positive or an adverse event affecting one sector will have cascading effects upon others.

Lifeline Sector: A lifeline enables the continuous operation of critical government and business services and is essential to human health and safety or economic security.

Mitigation: Ongoing and sustained action that eliminates or reduces the potential effects of hazards.

Resilience: Ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.

Security Risk Assessment: A process during which the assessor combines all the information on assets, threats/hazards, and vulnerabilities and then considers the potential impacts and prioritizes them based on the consequences of a loss event. Often expressed in the following formula: Risk = (Threat x Vulnerability x Impact).

Security Risk Management: Providing recommendations for countermeasures (i.e., security enhancements and risk mitigations) to reduce the assessed risks. This may also include risk transfer, risk avoidance, and risk acceptance approaches.

Threat: Indication of potential harm to life, information, operations, the environment and/or property; may be a natural or human-created occurrence.

Venue: As defined by the International Association of Venue Managers (IAVM), a venue is a "specific site, room, building, or facility where large events occur."

Vulnerability: A vulnerability is a physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard.

RESOURCES

Please visit cisa.gov for additional resources on dependencies, planning and preparedness efforts, vulnerability assessments, and other CISA tools and services.

1. **CISA Tabletop Exercise Packages (CTEP) | CISA**
   A webpage offering a comprehensive set of resources designed to assist stakeholders in conducting their own exercises. Partners can use CTEPs to initiate discussions within their organizations about their ability to address a variety of threat scenarios.
   CISA Tabletop Exercise Packages (CTEP) | CISA

2. **Community Systems Dependency Discussion Guide | CISA**
   A brainstorming worksheet to facilitate dependency discussions with the planning team, other participants, or stakeholder groups.
   Community Systems Dependency Discussion Guide | CISA

3. **Critical Infrastructure Sector Partnerships | CISA**
   A web page outlining the collaborative framework between the public and private sectors to safeguard critical infrastructure. It includes two councils: 1) SCCs, which are self-governed groups comprising owners, operators, trade associates, and industry representatives, and 2) GCCs, which consist of representatives from FSLTT governments.
   Critical Infrastructure Sector Partnerships | CISA

4. **Dependency Identification Worksheet | CISA**
   A worksheet that helps planning participants identify their facility's dependencies related to energy, communications, transportation, water, wastewater, cyber, and critical systems.
   Dependency Identification Worksheet | CISA

5. **Dependency Vulnerability Assessment | CISA**
   A web page offering three approaches to help community planners identify key infrastructure dependencies that present risks to fundamental services.
   Dependency Vulnerability Assessment | CISA

6. **Infrastructure Dependency Primer | CISA**
   A web resource that helps users learn about dependencies, plan for increased resilience, and implement mitigation measures and best practices.
   Infrastructure Dependency Primer | CISA

7. **Infrastructure Resilience Planning Framework | CISA**
   A web resource to help state, local, tribal, and territorial governments and associated regional organizations understand and plan for the resilience of critical infrastructure services.
   Infrastructure Resilience Planning Framework (IRPF) | CISA

8. **Mass Gathering Security Planning Tool | CISA**
   A tool providing event planners with a framework to begin or continue planning efforts for a mass gathering or special event and to connect stakeholders to the suite of tools and resources provided by CISA and its partners.
   Mass Gathering Security Planning Tool | CISA

9. **National Council of ISACs | NCI**
   A webpage offering details about Information Sharing and Analysis Centers (ISACs). ISACs are member-driven organizations that deliver all-hazards threat and mitigation information to asset owners and members.
   National Council of ISACs | NCI

10. **Office for Bombing Prevention – Planning and Preparedness | CISA**
    A web resource to help users leverage improvised explosive device (IED) risk landscape resources and learn about federal programs that help build and sustain bombing prevention preparedness.
    Planning and Preparedness | CISA

11. **Planning Participant Contact Information Worksheet | CISA**
    A template designed to organize and manage contact details of stakeholders involved in infrastructure resilience planning. It helps planners systematically track participant information such as names, roles, organizations, and contact details, facilitating efficient communication and collaboration across government and private sector groups.
    Planning Participant Contact Information Worksheet | CISA

12. **Public Safety Communications Dependencies on Non-Agency Infrastructure and Services | CISA**
    A white paper providing examples of infrastructure and service dependencies that public safety agencies might have on non-agency entities, with a goal of helping to secure system resilience and continuity of services.
    Public Safety Communications Dependencies on Non-Agency Infrastructure and Services | CISA

13. **Regional Services | CISA**
    A website outlining the regional services available through CISA's outreach program; includes Protective Security Advisors, Cyber Security Advisors, Emergency Communications Coordinators, and Chemical Security Inspectors. Regional personnel deliver risk and risk mitigation advice, conduct outreach, assessments and inspections, coordinate and deliver training and exercise support, and more.
    Find Help Locally | CISA

14. **Securing Public Gatherings | CISA**
    A webpage offering resources on how to connect with local authorities, develop incident response plans, train staff, and report concerns to emergency authorities.
    Securing Public Gatherings |CISA

15. **Security Advisors | CISA**
    A webpage providing information about field personnel who help to build stakeholder resiliency and form partnerships by assessing, advising, assisting, and providing a variety of risk management and response services.
    Security Advisors |CISA

16. **See Something, Say Something® | DHS**
    A webpage offering resources and information about DHS' "See Something, Say Something®" campaign.
    See Something, Say Something | DHS

17. **Stadium Spotlight: Connected Devices and Integrated Security Considerations | CISA**
    A web resource providing stadium owner and operators and security professionals with a snapshot of the connected stadium environment, key vulnerabilities and consequences, and recommended enterprise- and asset-level risk mitigations.
    Stadium Spotlight: Connected Devices and Integrated Security Considerations |CISA

18. **Venue Guide for Security Enhancements | CISA**
    A web resource and tool for venue operators that serves as a broad catalog to support safe and secure day-to-day operations and event management planning and execution.
    Venue Guide for Security Enhancements |CISA