

# U.S. Department of Homeland Security

Protective Security Coordination Division  
Office of Infrastructure Protection



## Infrastructure Protection Report Series

# Large Outdoor Public Gatherings

Large outdoor public gatherings include, but are not limited to, parades, fairs, festivals, rallies, farmer's markets, demonstrations, concerts, and celebrations. Unlike limited-duration events at fixed facilities, large outdoor public gatherings are not confined to a physical structure and do not rely on a permanent allocation of dedicated security resources. Rather, they usually rely on local law enforcement to provide security during the event. Nearly all aspects of security must be uniquely planned and formulated for each individual gathering. Large outdoor public gatherings are typically open-access events and have been successfully targeted by terrorists on numerous occasions in the past.



## Potential Indicators of Terrorist Activity

Terrorists have a wide variety of weapons and tactics available to achieve their objectives. Specific threats of most concern to large outdoor public gatherings include:

- Improvised explosive devices (IEDs)
- Vehicle-borne improvised explosive devices (VBIEDs)
- Chemical/biological/radiological agents
- Small arms attack

Terrorist activity indicators are observable anomalies or incidents that may precede a terrorist attack. Indicators of an imminent attack requiring immediate action may include the following:

- Persons wearing unusually bulky clothing that might conceal suicide explosives or weapons
- Suspicious or illegally parked vehicles near a gathering
- Unattended packages (e.g., backpacks, briefcases, boxes) that might contain explosives

- Persons attempting to gain unauthorized entry to the gathering or restricted areas
- Persons appearing to prepare to launch a standoff weapon (e.g., rocket-propelled grenades) at the gathering

Indicators of potential surveillance by terrorists include:

- Persons discovered with documents highlighting critical areas, infrastructure, or high-profile attendees
- Persons questioning event employees about practices pertaining to the gathering and its operations
- Event employees inquiring about operations or security measures; using video/camera/observation equipment; or possessing maps, photos, or diagrams that are not related to their jobs
- Event employees noted as willfully associating with suspicious individuals
- A noted pattern of false alarms, equipment failures, or power outages with indications of potential sabotage designed either to test the event operations response or to be part of an actual attempt to disrupt the event
- Theft or unauthorized possession of identification cards or uniforms
- Sudden losses or theft of guard force communications equipment
- Unusual and unexpected maintenance activities (e.g., road repairs) near the gathering site
- Displaced or misaligned manhole covers or other access doors on or surrounding the gathering site

## Common Vulnerabilities

The following are key common vulnerabilities of large outdoor public gatherings:

- Unrestricted public access to grounds and peripheral areas, such as parking lots
- Many access points with limited access control
- Temporary structures lacking safety features
- Limited security force or employee background checks
- Lack of exercises for emergency plans
- Multiple locations to place explosives or hazardous agents

## Protective Measures

Protective measures include equipment, personnel, and procedures designed to protect against threats and to mitigate the effects of an attack. Protective measures for large outdoor public gatherings include:

### • Planning and Preparedness

- Develop comprehensive security and emergency response plans and exercise periodically.
- Designate a security director to develop, implement, and coordinate all security-related activities.
- Maintain constant awareness of current threat conditions and available intelligence information.
- Develop policies and procedures for dealing with hoaxes and false alarms.
- Establish liaison and regular communications with local law enforcement and emergency responders.
- Keep records of all security-related incidents.
- Review and implement the pertinent recommendations from the FEMA Independent Study Program (FEMA IS-15) *Special Events Contingency Planning for Public Safety Agencies*.

### • Personnel

- Conduct background checks on security employees.
- Incorporate security awareness and appropriate response procedures for security situations into vendor and organizer employee training programs.
- Maintain an adequately sized, equipped, and trained security force.
- Provide an adequate level of security supervision and oversight for the event. Be alert to suspicious activities. Maintain awareness of any unusual patterns of illness that might indicate exposure to toxic agents.
- Coordinate security force operations with local law enforcement and possibly state and federal agencies.

### • Access Control

- Define an event or gathering perimeter if possible.
- Identify a buffer zone to restrict access to the event.
- Provide signage to restrict access to nonpublic areas.
- Provide security guards at access points.
- Prohibit entry of security-sensitive items.
- Use centralized parking and shuttle service.
- Remove any unauthorized vehicles.

### • Barriers

- Evaluate and install a perimeter barrier if warranted.
- Establish a clear zone around sensitive or critical facilities within the gathering area.
- Install barriers to separate vehicles from crowds.

### • Communication and Notification

- Install systems that provide communications with all people at the event, including employees, security force, emergency response teams, and visitors.
- Install systems that provide communications with local law enforcement and emergency responders.

- Develop a notification protocol that outlines who should be contacted in emergencies.
- Provide a simple and straightforward means for people to communicate the presence of a potential threat or an emergency.

### • Monitoring, Surveillance, Inspection

- Evaluate, design, and implement a monitoring, surveillance, and inspection program.
- Provide visual surveillance capabilities.
- Deploy the security force to regularly inspect sensitive or critical areas for signs of security issues.
- Monitor all people entering and leaving the event.
- Inspect packages, briefcases, backpacks, and parcels.
- Monitor any work adjacent to the event or gathering.

### • Infrastructure Interdependencies

- Ensure that the event has adequate utility service capacity to meet normal and emergency needs.
- As practical, locate gatherings a safe distance from hazardous areas or infrastructure (e.g., liquid fuel tanks, high-voltage power lines).

### • Incident Response

- Ensure that an adequate number of emergency responders are on duty and/or on call at all times.
- Develop policies and procedures for dealing with an incident to advise the public of the situation and to diffuse rumors and panic.

#### WARNING

This document is **FOR OFFICIAL USE ONLY (FOUO)**. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid “need-to-know” without prior approval of an authorized DHS official.

At a minimum when unattended, this document is to be stored in a locked container such as a file cabinet, desk drawer, overhead compartment, credenza or locked area offering sufficient protection against theft, compromise, inadvertent access and unauthorized disclosure.

*For more information about this document contact:  
Protective Security Coordination Division  
(IPassessments@dhs.gov or FOBanalysts@dhs.gov)*