U.S. Department of Homeland Security

Protective Security Coordination Division
Office of Infrastructure Protection

Infrastructure Protection Report Series

Public Institutions: Museums, Libraries, Zoos, Planetariums, Aquariums

There are more than 1,300 museums, 116,000 libraries, and 150 zoos and aquariums located in every state and region of the Nation. They range in size from large urban museums and libraries to small, one-story facilities in small towns and rural areas. Many include venues where people gather for shows, lectures, and other programs. Many large central libraries and smaller local libraries have meeting rooms and other areas where people congregate. Public institutions operate on the principle of open access and have limited in-place or available security measures.

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 museums, libraries, zoos, planetariums, and aquariums include those that involve:

- Small arms attack
- Improvised explosive devices (IEDs)
- Arson or incendiary attack
- Chemical, biological, or radiological 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 in crowded areas wearing unusually bulky clothing that might conceal suicide explosives or weapons
- Suspicious or illegally parked vehicles near buildings or where large numbers of patrons gather
- Unattended packages (e.g., backpacks, briefcases, boxes) that might contain explosives
- Persons or teams of people spotted in or around the facility attempting to gain unauthorized access to restricted areas
- Suspicious packages and/or letters received by mail
- Evidence of unauthorized access to heating, ventilation, and air-conditioning (HVAC) areas; indications of unusual substances near air intakes

Indicators of potential surveillance by terrorists include:

- Persons possessing or observed using observation equipment (e.g., cameras, binoculars, night-vision devices) near the facility over an extended period
- Persons discovered with maps, photos, or diagrams with facilities or sensitive areas highlighted
- Persons parking, standing, or loitering in the same area over an extended period with no reasonable explanation
- Persons questioning employees off-site about practices pertaining to the facility, especially security operations
- Employees changing working behavior or working more irregular hours without explanation
- Persons observed or reported to be observing facility receipts or deliveries
- A noted pattern or series of false alarms requiring a response by law enforcement or emergency services
- Unfamiliar cleaning crews or other contract workers
- Buildings or sensitive areas left unsecured
- Sudden losses or thefts of guard force equipment

Common Vulnerabilities

The following are key common vulnerabilities of museums, libraries, zoos, planetariums, and aquariums:

- Unrestricted public access
- Large crowds gathered in a single area
- Limited security force
- Multiple locations to place explosives or hazardous materials
- Limited employee background checks
- Presence and accessibility of items having unique symbolic value and/or significance

Protective Measures

Protective measures include equipment, personnel, and procedures designed to protect a facility against threats and to mitigate the effects of an attack. Protective measures for public institutions include:

- **Planning and Preparedness**
  - Develop comprehensive security and emergency response plans and conduct regular exercises of the plans.
  - Maintain a constant awareness of the current threat condition and available intelligence information.
  - Establish liaisons and regular communications with local law enforcement and emergency responders.
- **Personnel**
  - Conduct background checks on all employees.
  - Issue ID badges for all employees; require badges to be displayed at all times
  - Incorporate security awareness and appropriate response procedures for addressing security situations into training programs.
  - Maintain an adequately sized, equipped, and trained security force.
- **Access Control**
  - Provide appropriate signs to restrict access to nonpublic areas.
  - Identify and control access by all employees, vendors, delivery personnel, and contractors.
  - Install electronic access control systems and intrusion detection systems in sensitive areas.
  - Identify key areas in or next to buildings and prohibit parking in these areas.
- **Barriers**
  - Provide adequate locks, gates, doors, and other barriers for designated security areas.
  - Inspect barriers routinely for signs of intrusion.
  - Install barriers at HVAC systems, hatches, and power substations and routinely patrol these areas.
- **Communication and Notification**
  - Install, maintain, and regularly test the facility security and emergency communications system.
  - Communicate threat level information to employees.
  - Take any threat (phone, fax, e-mail) seriously.
  - Encourage employees and the public to report any suspicious activity that might constitute a threat.
- **Monitoring, Surveillance, Inspection**
  - Install closed-circuit television (CCTV) systems, intruder alarms, and lighting to cover key areas.
  - Train security personnel to watch for repeated visitors who have no apparent business in the facility, unusual activities, abandoned packages, and to monitor utility supplies and routine work activities scheduled on or near assets.
  - Conduct regular inspections of lockers, mail room areas, trash bins, parking lots, garages, and all designated security areas under access control.
  - Consider using night vision/infrared CCTVs to monitor areas requiring dim lighting (e.g., theatres, shows, and zoo/aquarium dark habitat facilities).
- **Infrastructure Interdependencies**
  - Provide adequate security and backup for critical utility services (e.g., electricity, natural gas, water, telecommunications)
  - Locate fuel and utility supply facilities at a safe distance from buildings and high-traffic areas.
- **Cyber Security**
  - Implement and review hardware, software, and communications security for computer-based operational systems.
  - Eliminate any information that might provide security information to adversaries from the Web site.
- **Incident Response**
  - Develop and maintain an up-to-date emergency response plan.
  - Prepare an emergency operations center to coordinate resources and communications during an incident.
  - Review unified incident command procedure for responding to an event with local law enforcement and emergency responders and government agencies.

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)