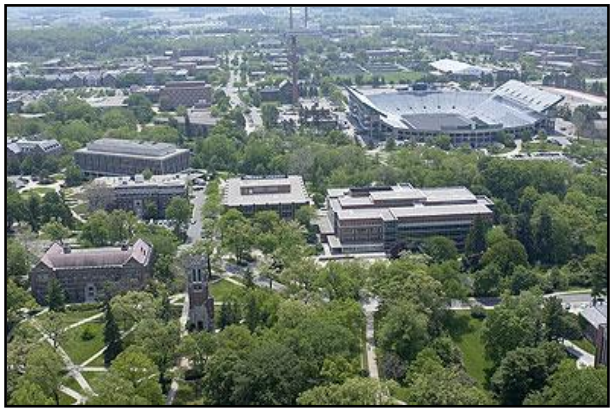
U.S. Department of Homeland Security

Protective Security Coordination Division
Office of Infrastructure Protection

Infrastructure Protection Report Series

Higher Education Institutions

The higher education community in the United States consists of more than 11,000 higher education institutions that collectively serve more than 17 million students, employ more than 3.4 million faculty and staff, and have combined budgets approaching $360 billion. Higher education institutions range in size from small institutions with fewer than 100 students to large universities with tens of thousands of students and faculty occupying campuses the size of a small town or city. Institution grounds are generally open-access, with varying levels of security within the campus.



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 higher education institutions include:

- Small arms attack
- Improvised explosive devices (IEDs)
- Chemical or biological attack
- Arson or incendiary attack

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

- Persons wearing unusually bulky clothing that might conceal suicide explosives or weapons
- Persons or teams of people attempting to gain unauthorized access to restricted areas
- Suspicious or illegally parked vehicles near institution facilities or where crowds gather
- Unattended packages (e.g., backpacks, briefcases, boxes) that might contain explosives or hazardous materials
- 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 using observation equipment (e.g., cameras, binoculars, night-vision devices) near institution facilities or grounds over an extended period
- Persons parking, standing, or loitering in the same area over an extended period with no reasonable explanation
- Persons discovered with maps, photos, or diagrams with institution or key facility components highlighted
- Employees whose working behavior has changed or who are working more irregular hours
- Persons questioning employees or students about the institution's operations, especially security measures or practices
- Unfamiliar service or contract personnel with passable credentials attempting to access unauthorized areas

Common Vulnerabilities

The following are key common vulnerabilities of higher education institution:

- Generally open access to students, faculty, staff, and public
- Limited or no vehicle access or content control
- Building designs that are not security-focused; subsequent vulnerability to explosives, arson, chemical/biological contaminants introduced into HVAC systems, blocked emergency exits, etc.
- Congregation of large numbers of people, especially for events (concerts, athletic events, lectures) with levels of security and screening ranging from none (e.g., for regular class lectures) to tight (e.g., for high-profile athletic competitions)
- At institutions with research programs, presence on campus of hazardous chemical, biological, or radiological materials with widely varying levels of security

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 higher education institutions include the following:

- **Planning and Preparedness**
  - Develop a comprehensive security and emergency response plan. Coordinate the plan with appropriate agencies. Conduct regular exercises of the plan.
  - Establish liaison and regular communication with local law enforcement and emergency responders.
  - Establish procedures to implement additional protective measures as the threat level increases.
- **Personnel**
  - Conduct background checks on all employees.
  - Review the personnel files of recently terminated employees to determine whether they pose a security threat.
  - Incorporate security awareness and response procedures into employee/student training programs.
  - Require contractors, vendors, and employment agencies to vouch for the background and security of their personnel who will work at the facility.
- **Access Control**
  - Restrict parking to areas away from critical assets.
  - Maintain strict control of personnel access into critical or sensitive areas.
  - Identify a buffer zone extending out from the institution that can be used to further restrict access to facilities when necessary. Coordinate with local law enforcement and U.S. Coast Guard on buffer zone protection measures as appropriate.
  - Limit access to contractors, vendors, and temporary employees who are expected and whose presence has been confirmed by prior arrangement.
- **Barriers**
  - Provide adequate locks, gates, doors, and other barriers for designated secure areas. Inspect barriers routinely for signs of intrusion.
  - Install barriers at HVAC systems, hatches, and power substations. Routinely patrol these areas.
- **Communication and Notification**
  - Install, maintain, and regularly test security and emergency communication systems. Ensure functionality and interoperability with local law enforcement.
  - Encourage employees, students, and the public to report any suspicious activity that might constitute a threat.
- **Monitoring, Surveillance, Inspection**
  - Install and regularly test alarms and intrusion detection systems at critical areas and the institution perimeter. Coordinate with law enforcement.
  - Monitor the activities of on-site contractors and vendors. Inspect all work before releasing them.
  - Monitor building exits to assure functionality in emergency situations.
- **Infrastructure Interdependencies**
  - Ensure that the institution has adequate utility service capacity to meet normal and emergency needs.
  - Where practical, provide for redundancy and emergency backup capability.
- **Cyber Security**
  - Implement adequate policies, procedures, and culture regarding cyber security.
  - Eliminate any information from the institution's Web site that might provide security information to adversaries.
  - Validate the credentials and work of contractors and vendors given access to technology systems.
  - Immediately cancel access for terminated staff.
  - Control physical access to critical technologies.
- **Incident Response**
  - Develop and maintain an up-to-date emergency response plan, incident notification process, and emergency calling trees that cover all staff.
  - Prepare an emergency operations center to coordinate resources and communications during an incident.

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, or credenza, or a 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)