U.S. Department of Homeland Security

Protective Security Coordination Division
Office of Infrastructure Protection

Infrastructure Protection Report Series

Elementary and Secondary Schools

Approximately fifty million students attend nearly 100,000 public elementary and secondary schools throughout the Nation. Elementary and secondary schools are relatively open-access, limited egress congregation points for children, and have been successfully targeted by terrorists 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 schools include:

- Small arms attack
- Improvised explosive devices (IEDs)
- Vehicle-borne improvised explosive devices (VBIEDs)
- Arson or incendiary attack
- Chemical or biological 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 (e.g., school auditorium, cafeteria, athletic facilities) wearing unusually bulky clothing that might conceal suicide explosives or weapons
- Vehicles approaching the school at an unusually high speed or steering around barriers and traffic controls
- Suspicious or illegally parked vehicles on or near school grounds
- Unattended packages (e.g., backpack, briefcase, box) that may contain explosives. Packages may be left in open areas or may be hidden in trash receptacles, lockers, or similar containers.
- Evidence of unauthorized access to heating, ventilation, and air-conditioning (HVAC) areas of a school; indications of unusual substances near air intakes
- Suspicious packages and/or letters received by mail that might contain explosives or chemical/biological/ radiological agents.

Indicators of potential surveillance by terrorists include:

- Persons using or carrying video/camera/observation equipment in or near the school over an extended period
- Persons parking, standing, or loitering in the same area over a multiple-day period with no reasonable explanation
- Persons questioning school employees off-site about practices pertaining to the school and its operations
- Persons discovered with school maps, photos, or diagrams with key components or sensitive areas highlighted
- Suspicious personal e-mail, telephone, fax, or postal mail requests for information about the school or its operations
- A noted pattern of false alarms requiring a response by law enforcement or emergency services
- Threats by telephone, mail, or e-mail and/or increase in reports of threats from known reliable sources

Common Vulnerabilities

The following are key common vulnerabilities of elementary and secondary schools:

- Relatively open access to school grounds and buildings
- Limited or no vehicle access controls
- Large concentrations of students gathering in open areas outside school buildings on a regular and readily observable schedule
- Proximity of schools and neighboring facilities, especially in urban areas
- Limited or no inspection of students' personal articles, particularly in lower-crime areas
- Limited security on school buses

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 elementary and secondary schools include:

- **Planning and Preparedness**
  - Designate an employee as security director to develop, implement, and coordinate all security-related activities
  - Conduct security audits on a regular and continuing basis. Develop a comprehensive security plan and emergency response plan for the school
  - Conduct regular exercises of emergency plans
  - Establish liaison and regular communication with local law enforcement and emergency responders
- **Personnel**
  - Conduct background checks on all school employees
  - Incorporate security into employee training programs
  - Provide security information and training to all students
- **Access Control**
  - Define the facility perimeter and areas within the facility that require access control. Maintain building access points to the minimum needed
  - Issue photo identification badges to all school employees and students
  - Require visitors check in with the front office upon arrival and departure
  - Provide visitors with school issued identification badges when on school grounds.
  - Positively identify all vehicles and drivers that enter the school parking lots
  - Institute a policy restricting other vehicles from accessing the bus-loading zone
  - Secure ladders, awnings, and parapets that provide access to building roofs, HVAC systems, and other critical equipment
- **Barriers**
  - Install appropriate perimeter barriers and gates. Maintain clear area at perimeter barriers to enable continuous monitoring and to inhibit concealment of people or packages
  - Establish a clear zone adjacent to buildings. Keep zone free of vegetation and other obstructions
  - Install barriers to protect doors and windows from small arms fire and explosive blast effects
- **Communication and Notification**
  - Install system(s) that provide communication with all people at the school, including employees, students, emergency response teams, and visitors
  - Develop a plan for communicating with parents during emergency situations
  - Develop a notification protocol that outlines who should be contacted in emergencies.
  - Develop a procedure for communicating with the public and the media regarding security issues
- **Monitoring, Surveillance, Inspection**
  - Evaluate needs and design a monitoring, surveillance, and inspection program
  - Provide visual surveillance capability (e.g., designated surveillance points, cleared lines of sight)
  - Install intrusion detection and alarm systems
  - Deploy personnel assigned to security duty to regularly inspect sensitive or critical areas
  - Continuously monitor all people entering and leaving the facility for suspicious behavior
  - Continuously monitor all vehicles approaching the facility for signs of threatening behavior
- **Infrastructure Interdependencies**
  - Ensure that the school has adequate utility service capacity to meet normal and emergency needs
  - Ensure that employees are familiar with how to shut off utility services
  - Provide adequate physical security for utility services
- **Cyber Security**
  - Develop and implement a security plan for computer and information systems hardware and software
  - Maintain a well-trained computer security staff
- **Incident Response**
  - Ensure that an adequate number of emergency response personnel are on duty and/or on call
  - Provide training and equipment to emergency response personnel to enable them to deal with terrorist-related incidents
  - Check the status of all emergency response equipment and supplies on a regular basis
  - Develop a plan for discharging students following incident resolution

For more information about this document contact:
Protective Security Advisor Duty Desk
(IPassessments@dhs.gov or FOBanalysts@dhs.gov)