Infrastructure Series|School Security

New Jersey Regional Operations and Intelligence Center (ROIC) ~ ROIC202205-13022X
7 June 2022

Key Finding

The goal is to strengthen the defenses of a school campus, deterring criminal or terrorist activity by increasing the perceived risk to an offender. The perception of difficulty or presence of obstacles to complete a criminal act promotes deterrence. Escalating the time required to conduct an illicit action increases the likelihood of apprehension, thereby deeming the target undesirable. Listed below are School Security Preparedness and Protective Measures best practices designed to Deter, Detect, Delay, and Defend against incidents involving school violence.

Preparedness

- **Assessment:** Conduct an annual school safety and security assessment of the school campus and building(s) in coordination with your local Law Enforcement, Counter Terrorism and Critical Infrastructure Coordinators.
- **Mapping:** Obtain digital mapping of the facility and surrounding vicinity. Schools present unique challenges to emergency responders due to their size, complexity and occupants. Responders require extensive yet easily understandable information in the event of an attack or other emergency at a school. Districts should ensure that each facility can provide an overall floor plan, a roof plan, fire, HVAC, security systems and other emergency information useful to police, fire and other emergency partners. At a minimum, this information should include:
    - All room names and associated numbers;
    - A minimum five-block radius outside the school property perimeter;
    - Identification of security cameras and other access control devices.

  (Partner Alliance for Safer Schools 2018, Pg. 35 Facility and Vicinity Mapping)
- **Doors:** Number all exterior entrances. Marked entrances should conform to a uniform numbering system (e.g., the main entrance is #1, numbering clockwise from there) to assist emergency responders in locating particular areas. (New Jersey School Security Task Force Report and Recommendations-2015, Chapter 4.12 Hardening School Perimeters and Building Entryways)
- **Stairwells:** Each stairway should be identified and its designation posted inside and on the outside all doors leading to the stairs.
- **Windows:** The numbering of exterior windows and the interior of rooms corresponding with the designated room number assists first-responders in quickly locating people during an emergency such as an active shooter. Originally developed for schools, this practice can provide benefits for all occupied buildings during emergencies. (FEMA 426, 2.6)
- **Safe Zones:** In regards to school safety and security, establish safe zones or hard corner is an area of the classroom that cannot be seen by someone looking through a window(s). It does not mean the area is reinforced with any protective materials or barriers. (Marjory Stoneman Douglas High School (Parkland Florida) Public Safety Commission Initial Report, pgs. 36-37 January 1, 2019)

- **Training:** Conduct training and scenario-based exercises together to clearly define emergency response roles and responsibilities. Training for school safety personnel should include bullying, hazing, truancy, Internet safety, emergency planning, emergency drills, drugs, weapons, gangs and school policing, and any other areas deemed necessary. (N.J.S § 18A:17-43.2)
- **Emergency Plans:** Policies and procedures component involves a school or district's emergency operations plan (EOP) and security plans. Comprehensive security plans, and the policies and procedures created to implement them, form the foundation of school safety and security. Without proper policies and procedures in place, it is impossible to successfully use security technology and other security measures, regardless of how advanced they may be. Effective policies and procedures alone can mitigate risks, and there are often no costs associated with implementing them. (Partner Alliance for Safer Schools 2018, Pg.13, Policies and Procedures)
- Copies of each school or site plan should be distributed as follows:
    - One copy to every staff member at the beginning of each school year. Special attention must be given to providing site plans to substitutes, volunteers, itinerant personnel, and new staff.
    - One copy filed in each Emergency Procedures manual issued to the site.
    - One copy included in the site safety plan sent to local law enforcement.

  (School Safety and Security, Best Practice Guidelines, New Jersey Department of Education, December 2006, page 110.)
- The chief school administrator shall consult with law enforcement agencies, health and social services provider agencies, emergency management planners and school and other community resources, as appropriate, in the development of the school district's plans, procedures and mechanisms for school safety and security. (N.J.A.C. 6A:16-5.1)
- **Communication:** Communication systems with visual indicators for specific hazards. Providing more than one form of communication (audible) during an emergency event is preferred. Ensure the communication system is audible in all interior and exterior locations. Using visual indicators outside the building allows students and staff awareness of a threat through a different sense. According to the NFPA, both audible and visual cues to alert persons are essential to communicating a threat. Enhanced implementations accomplish this through color-coded visual cues that correspond to specific types of threats. (Partner Alliance for Safer Schools 2018, Pg.52, Visual Indicators Specific to Hazard) Provide clear and concise communication among law enforcement, faculty, students, and the public during and after an incident
- **Security Forces:** School districts should enter into a written agreement with local law enforcement agencies stipulating the terms and conditions governing placement of security personnel in school buildings. The agreement should address matters including, but not limited to: the chain of command; roles and responsibilities of security personnel while on school property; work hours and conditions; required qualifications and experience; channels of communication; required training and continuing professional development; and authority to carry firearms. (School Safety and Security, Best Practice Guidelines, New Jersey Department of Education, December 2006, page 43.)
- **Emergency Building Access for Fire/Law Enforcement:** A "Knox Box" type system should be installed. The system holds a master key or credential accessible only to fire

departments, emergency medical services and law enforcement, allowing rapid access to locked doors in emergencies. Consider installing separate boxes for fire and law enforcement. (Partner Alliance for Safer Schools 2018, Pg. 70)

- **Interdependencies:** Install systems for redundancy in power generation and distribution systems for the facility. Measures include redundant power feeds, emergency generators, and Uninterruptible Power Supplies. Size the generator appropriately; ensuring the facility maintains uninterrupted critical functions in the event of power outages. Implement a policy requiring the periodic testing of emergency equipment. (ASIS International 2009, Chapter 3.2.2. Site Hardening)

Cybersecurity: On October 8, President Joe Biden signed the K-12 Cybersecurity Act into law to enhance the cybersecurity of K-12 institutions in the United States. This law highlights the significance of protecting the sensitive information maintained by schools across the country. This law is an important step forward to meeting the continuing threat posed by criminals, malicious actors, and adversaries in cyberspace. Details of the K-12 Cybersecurity Act of 2021 can be found here. The below sections will address best practices for device security and email and account security:

- **Device Security:** Use approved resources and platforms. Keep hardware and software, including mobile device operating systems and applications, up to date. Run an updated anti-virus/anti-malware program. Check privacy and security settings. Backup devices. Secure physical devices and cover and/or disconnect your camera when not in use.
- **Email and Account Security**: Identify common red flags, like poor grammar and spelling, and unexpected requests. Refrain from clicking links or opening attachments from unknown senders. Confirm the legitimacy of emails from known senders that request sensitive information by contacting the sender via a separate means of communication. Manually type URLs into browsers. Refrain from sharing login credentials or other sensitive information. Use unique, complex passwords for all accounts and enable multifactor authentication (MFA) where available. Update passwords immediately following a data breach or potential compromise. Use the NJCCIC instructional guides to implement security and privacy controls. Review and apply recommendations found in the NJCCIC post How Big is Your Footprint?

We encourage users to report cyber incidents immediately to all associated online platforms, the Federal Trade Commission (FTC) at ReportFraud.ftc.gov, and the NJCCIC Cyber Incident Report Form accessible at www.cyber.nj.gov.

PHYSICAL SECURITY ENHANCEMENT SUGGESTIONS

Perimeter

- Use the Crime Prevention through Environmental Design (CPTED) principle of "territorial reinforcement," clearly designating school property. Fencing, plantings, berms or a blend of all three will discourage trespassers
- School districts should assign security patrols and/or encourage law enforcement to have patrolling officers, discouraging trespassing and other unwanted activities.
- Separate bus drop-off/pick-up areas from other vehicular drop-off/pickup areas. (School Safety and Security, Best Practice Guidelines, New Jersey Department of Education, December 2006, page 47.)

Lighting

- Conduct annual assessment of safety and security lighting based upon industry and local standards. Security and parking lot lighting should be a minimum lighting level of 2.00 (fc) for open areas and 0.50 (fc) for the outer perimeter. Reduce areas of concealment created by low light conditions by overlapping and continuous lighting. Establish a maintenance program inspecting and replacing light fixtures and bulbs at 80% of their recommended life. (Illuminating Engineers Society of North America 23-24)

Barriers

- Install bollards along walkways and areas of mass gathering, mitigating the effects of an accidental or intentional incident involving a motor vehicle. Bollards are available in configurations meeting the ASTM International standards. ASTM F2656 standard includes penetration levels of P1, P2, and P3. (U.S. Department of Transportation, Federal Highway Administration 2018, Chapter 5 Vehicle Security Barrier Performance Standards)
- Bollard spacing should be between 36 and 48 inches, depending on the kind of traffic expected and the needs of pedestrians, people with strollers and wheel chairs, and the elderly. In long barrier systems, bollards should be interspersed with other streetscape elements such as hardened benches, light poles, or decorative planters. Keep bollards clear of Americans with Disabilities Act (ADA) access ramps and the corner quadrants at streets. (U.S. Department of Transportation, Federal Highway Administration 2018, Chapter 6.4.2 Passive Bollards)
- Install traffic-calming methods, such as raised crosswalks or speed bumps, to reduce the maximum possible speed of a vehicle approaching the recess area. (U.S. Department of Transportation, Federal Highway Administration 2018, Chapter 3.3 Traffic Calming)

Signage

- Install signage along the boundary of school grounds, sending an unambiguous message regarding hours (if any) when the public is welcome. Clearly define the property perimeter with signage stating that entry onto school property is limited to authorized visitors and those on official school business. If the public uses school grounds after school hours, signage should include hours the grounds are open to the public, and note activities and items that are prohibited
- Install wayfinding signage. Signs for vehicular and pedestrian circulation are an important

element of security. Signs clarify entries and routes for pedestrians, staff, visitors, deliveries, and service, each with specific functional objectives and security requirements. Design signage to keep intruders out of restricted areas. (FEMA 2007, FEMA 430: Site and Urban Design for Security 5-22)

- Install "No Trespassing" signage. Adequate "No Trespassing" signage deters unauthorized access to the facility. Place signs in multiple exterior locations, clearly indicating that no trespassing is permitted
- Install video surveillance signage advising visitors the property is under video surveillance

Parking

- Maintain a parking decal or tag system for all staff and students who park on campus, ensuring easy identification of unauthorized vehicles on the property. (School Safety and Security, Best Practice Guidelines, New Jersey Department of Education, December 2006, page 36.)
- Implement and enforce a policy requiring visitors to park in designated parking lots. Eliminating or restricting parking along the curb of the facilities increases standoff distance.
- Consider high-mast lighting for the parking lot areas, providing broader, more natural light distribution, and fewer poles. (ASIS International, 2009, Chapter 3.4.3 Equipment)

MIDDLE LAYER

Intrusion Detection Systems

- Each school building should be secured to protect against external threats when the building is unoccupied. Recommended intrusion detection systems include those using door position and latch bolt switches at each exterior door. In addition, large exterior windows that could provide easy entry to the building should be monitored using glass break detection devices. The intrusion detection system should have a minimum of one keypad used to arm and disarm the system. The intrusion system should also include alarms installed throughout the main areas of the building that sound when the intrusion system has an alarm. These alarms are the first points of deterring a threat once unauthorized entry to the building has occurred. (Partner Alliance for Safer Schools, 2018, p. 75)
- Every school building should have the intrusion system report to a central monitoring station; this allows first responders to be made aware of a possible intrusion into the school building. The monitoring of the system should be via a hardwired telephone line, IP connection or cellular type dialer

Video Surveillance

- Consult with industry experts, conducting a camera survey and for strategic installation of exterior/interior video surveillance coverage throughout the facility, focusing on the perimeter, ingress/egress corridors, hallways, classrooms, and other sensitive areas, to eliminate voids in interior and exterior video surveillance coverage.
- Ensure active monitoring of the video surveillance system. An unmonitored system merely documents events, and does not provide increased warning or command and control

during incidents. Provide remote access to the video feed to key administrators, stakeholders, and local law enforcement.

- Install large television monitors in administrative common areas, ensuring all staff members are able to view video surveillance footage, and increasing the number of stakeholders actively monitoring the facility.
- Install intercom systems at main entrances. Intercoms enable facilities to speak with and observe visitors at access point(s) prior to entering the facility. Intercoms integrated with an electronic access control system enables screeners to unlock the door remotely. Integrate intercom systems into the video surveillance system upon initiation and activation of two-way communication. (Partner Alliance for Safer Schools, 2018, p. 73)
- Video surveillance systems should have a retention period of a minimum of 30 days. (Department of Defense Education Activity 2015, Chapter 8.2 Closed Circuit Television Systems)
- Select video surveillance system equipment utilizing a systems approach rather than a components approach. A systems approach results in a video system that operates effectively. Buying components separately often results in a system that does not perform as expected or performs inefficiently

INNER LAYER

Access Control

- Design schools with a single public entrance used during the school day, equipped with a security vestibule with interior doors that school security or other staff release. The entry should be a secured vestibule with a mechanical lock or exit device.
- Exterior doors, and most doors in a school, should never be left unattended in the open position. These doors should all be equipped with commercial grade automatic closing hardware. Solid core doors offer much higher protection from forced entry and projectiles. All doors in the building should be solid core doors. (New Hampshire, Division of Homeland Security, School-Security-Standards, June 2014, B. Access Control, B-10, p4.)
- Use ballistic or shatter resistant film for glass entrance doors and sidelights and other vulnerable first floor areas. Fragment Retention Film (FRF) adheres to the interior surface of the glass and strengthens structural integrity. Film provides varying degrees of protection against intrusion and reduces injury from projectile shards of glass in case of an explosion. FRF is the most economical retrofit measure to strengthen the exterior glazed elements of the façade and FRF is most effective when used with a blast-tested anchorage system. Mechanical attachment systems and wet glazing techniques can be used to attach the FRF to the frame and reduce the likelihood of the glass separating from the frame. 7-mm-thick film or specially manufactured 4-mm-thick film is the minimum thickness that is required to provide hazard mitigation from a blast. (U.S. Department of Homeland Security 2011, 3-73, New Jersey School Security Task Force Report and Recommendations-2015, pg34)

Interior Doors

- Install shades on all room windows. During a lock down event, shades block the view of students and staff from the corridors by an aggressor. (N.J. Department of Education, Safety and Security Manual, Best Practices Guidelines, December 2006, p. 152.)
- Classrooms should be always locked. In the event of a lockdown, there would be a delay in locking down due to teachers having to lock their doors. (N.J. Department of Education, Safety and Security Manual, Best Practices Guidelines, December 2006, p. 152.)
- Keep unoccupied rooms and spaces locked when not in use. This practice requires full cooperation by faculty and staff. See the NCEF publication *Door Locking Options in Schools* for limitations on locking devices. (Low-Cost Security Measures for School Facilities, National Clearinghouse for Educational Facilities, April 2008.)
- Interior door shades should be drawn, the classroom lights off and the room locked in any unoccupied room. In the event of an intrusion, the aggressor would be unable to determine an occupied room from an unoccupied room
- All classroom doors shall be lockable from the inside without requiring lock activation from the hallway, and door locks shall be tamper resistant. (Final Report of the Sandy Hook Advisory Commission; State of Connecticut, March 6, 2015)

Visitor Management

- Implementing an electronic visitor management system assists schools in maintaining a record of who enters the building. School staff scan forms of identification, such as driver's licenses and other state identification cards. Electronic management systems offer efficiencies and protection against unauthorized visitors. (Cybersecurity & Infrastructure Security Agency 2022, K-12 School Security Guide, Chapter 3.3 Physical Security at Building Perimeter Layer)
- Screening systems include vehicle and package inspection, search of persons and bags, and metal detectors. Decisions regarding the employment of screening systems should be at the discretion of school districts, commensurate with local resources and security assessment. School districts should develop the appropriate procedures for staff training and equipment use.
- Every school should have a visitor badging system. Systems range from basic to advance. At a minimum, issue visitor badges to all individuals who are not staff or students. Sign all visitors in to a log using the visitors' government-issued identification cards and checking the student information system, ensuring that visitors are allowed on campus. Each visitor should be issued a badge that includes:
    - School name and logo;
    - Text that says "VISITOR" in large, bold font;
    - Name of visitor;
    - Expiration date and time;
    - Color code allowing staff to easily identify the type of visitor (e.g., parents are green, vendors are blue, volunteers are yellow).

    (Partner Alliance for Safer Schools 2018, Pg. 26, Vistor Badging System)

- Security enhancements are based on the noted industry standards and best practices. Implementing them should take into account federal, state, and local laws, codes, and ordinances.

References

1. ASIS International. (2009). *Facilities Physical Security Measures* .
2. Cybersecurity & Infrastructure Security Agency. (2022). K-12 School Security Guide.
3. FEMA. (2007). FEMA 430: Site and Urban Design for Security.
4. Illuminating Engineers Society of North America. (2014). Lighting for Parking Facilities.
5. Marjory Stoneman Douglas High School Public Safety Commission. (2019). *Marjory Stoneman Douglas High School Public Safety Commission Initial Report.*
6. New Jersey School Security Task Force. (2015). *Report and Recommendations.*
7. Partner Alliance for Safer Schools. (2018). Safety and Security Guidelines for K-12 Schools.
8. Sandy Hook Advisory Commission. (2015).
9. U.S. Department of Homeland Security . (2011). Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings.

Contact Information: *Any questions about this product should be directed to the Office of the ROIC Infrastructure Protection Unit at (609) 963-6900 or NJROICIPU@.njsp.org.*

Suspicious Activity Reporting: *Suspicious activity with a possible nexus to terrorism, as well as any threats of violence to schools, should be reported to NJOHSP CT Watch at 866.4SAFENJ (866.472.3365) or tips@njohsp.gov.*