PASS™
Partner Alliance
for Safer Schools

SAFETY AND SECURITY
GUIDELINES
for K-12 Schools

Clerk's Copy   1-16-2020

CONTENTS

DISCLAIMER: The *Safety and Security Guidelines for K-12 Schools* (the "Guidelines") are provided for informational purposes only. The individual contributors to the Guidelines, th employers, the organizations participating in the Partner Alliance for Safer Schools (PASS) and PASS itself make no warranties or guarantees regarding the information conta in the Guidelines, and expressly disclaim all liability for damages of any kind arising out of the use, reference to or reliance on the information contained in the Guidelines. Th Guidelines are not a substitute for expert professional advice that may be required to address the specific facts and circumstances related to the implementation of a particu school safety security measure or program.

PASS™
Partner Alliance for Safer Schools

About PASS

The Partner Alliance for Safer Schools (PASS) has a singular focus: To provide school administrators, school boards and public safety and security professionals with guidelines for implementing a layered and tiered approach to securing and enhancing the safety of school environments.

Established in 2014, PASS brings together expertise from the education community, law enforcement and the security industry to develop and support a coordinated approach that can assist school administrators in making effective use of proven security practices specific to K-12 environments and informed decisions on security investments.

In 2015, PASS first released the *Safety and Security Guidelines for K-12 Schools* (the "Guidelines"), which remains the most comprehensive information available on best practices specifically for securing school facilities available. The fourth edition (2018) is greatly expanded to address the growing range of complex security challenges facing today's K-12 schools, providing a resource for school officials—and their solutions providers—to help achieve the most appropriate and cost-effective deployment of security solutions. For more information, visit passk12.org.

Introduction

Today's school safety and security challenges are multifaceted and complex. There is no single action that will, by itself, make our schools safe. Protecting students and staff is a tremendous moral and legal responsibility that requires a comprehensive approach to these challenges.

Sadly, our nation's schools have increasingly become soft targets for mass violence. Since 2000, schools have been the second most frequent targets in active shooter incidents as defined by the FBI. The highly publicized mass murders at Columbine High School, Sandy Hook Elementary School and Marjory Stoneman Douglas High School and mass shootings at other schools have led to reassessments of how we manage risk in the K-12 environment in the 21st century. In a nation where approximately 56 million students attend nearly 132,000 K-12 schools, a rate of 37 active shooter incidents from 2000 to 2017[1] is, thankfully, an extremely low one. While this low-probability/high-consequence threat cannot be ignored, it should always be considered within the full picture of K-12 safety and security challenges.

Solutions to these challenges must be pursued across all areas of emergency preparedness: prevention, protection, mitigation, response and recovery; however, a modern and effective security infrastructure is a central component of any comprehensive school safety strategy. When other prevention efforts fail, facility security measures are critical to protection, mitigation and response.

Security management is a core responsibility of school administrators, who face daily pressure to ensure that students are protected, often without significant security expertise or the benefit of full-time safety/security staff. When it comes to security, administrators face two simple but difficult questions:

- What should we do?

- How do we prioritize?

The PASS Guidelines were developed to provide administrators with a means to effectively evaluate security infrastructure currently in place, prioritize investments and maximize security gained by leveraging available resources. The Guidelines identify and classify best practices for securing K-12 facilities in response to urgent needs for information identified by the education community:

- Specific actions that can effectively raise the baseline of security

- Vetted security practices specific to K-12 environments

- Objective, reliable information on available safety and security technology

- Assessment of current security measures against nationwide best practices

- Multiple options for addressing security needs identified

- How to distinguish needed and effective solutions from sales pitches on unnecessary products

---

[1] https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-incidents-graphics

PASS
Partner Alliance
for Safer Schools

Scope

The primary focuses of the PASS Guidelines are physical security and life safety, and recommendations are limited to related policies, procedures, equipment and technology. The Guidelines do not address other aspects of prevention often associated with school safety, such as mental health, behavioral threat assessment[2] or policies related to firearms. Likewise, many areas of response and recovery are the purview of law enforcement and other emergency responders. Great care has been taken to ensure consistency with and avoid unnecessary duplication of important recent work in these areas, such as the National Fire Protection Association's (NFPA's) *NFPA 3000 Standard for an Active Shooter/Hostile Event Response (ASHER) Program*,[3] released in 2018, which focuses in large part on response and recovery.

The Guidelines do not include best practices for deployment of security personnel, school resource officers and school-based policing. While these individuals play a critical role in securing school facilities, organizations like the National Association of School Resource Officers provide excellent resources on the issues and best practices that are specific to personnel.[4]

The Guidelines do not address every risk and every situation and, importantly, **do not include product-specific recommendations**. PASS does not endorse specific products, services or service providers. Further, the Guidelines do not address what may be considered "offensive" countermeasures, tactical equipment or arming staff or security personnel, as there is a lack of nation wide consensus on these issues in the K-12 environment at this time.

---

[2] Enhancing School Safety Through a Threat Assessment Model, U.S. Secret Service (2018), https://www.secretservice.gov/data/protection/ntac/USSS_NTAC_Enhancing_School_Safety_Guide_7.11.18.pdf

[3] https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=3000

[4] https://nasro.org/membership/resources/

Structure of the PASS Guidelines

Layered Security

The security profession and industry has always recognized that the best approach to security is a layered approach. Consistent with the practice of implementing security in depth and the site security approach recommended by the U.S. Department of Homeland Security (DHS),[5] the Guidelines describe approaches within five physical **layers** for school facilities.

LAYERS OF PROTECTION

- DISTRICT-WIDE
- PROPERTY PERIMETER
- PARKING LOT PERIMETER
- BUILDING PERIMETER
- CLASSROOM/INTERIOR PERIMETER
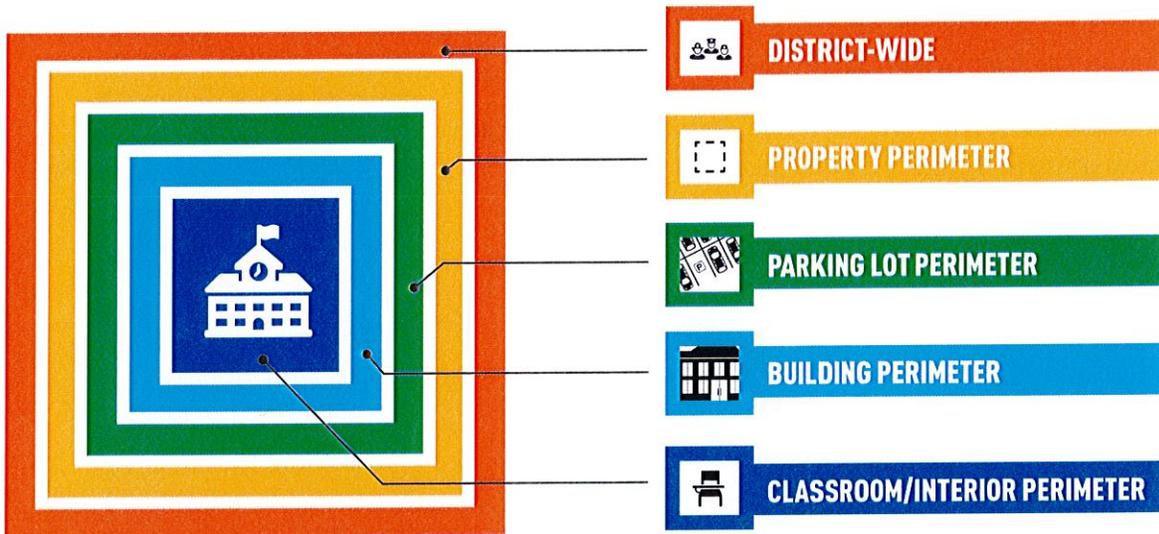
A layered approach is essential to addressing a broad range of threats, as each successive layer provides specific components to deter, detect or delay adversarial behaviors in the event that other layers are bypassed or breached. Each layer includes basic protective elements, or **components**, of security. Every layer does not necessarily include all seven of these common components, and a layer may include additional components unique to that layer.

SAFETY AND SECURITY COMPONENTS

- Policies and Procedures
- People (Roles and Training)
- Architectural
- Communication
- Access Control
- Video Surveillance
- Detection and Alarms

[5] DHS Primer to Design Safe Schools Projects (2012), dhs.gov/xlibrary/assets/st/bips07_428_schools.pdf

PASS
Partner Alliance
for Safer Schools

While components are not listed in a priority order, three components included in *all* layers are policies and procedures, the roles and training of people and communication. These components often perform a function in *every* layer and *every tier* in each layer.

CLASSROOM/INTERIOR PERIMETER	TIER 1	TIER 2	TIER 3	TIER 4
• COMMUNICATION				
» Public Address System	✔	✔	✔	✔
» E-911 Added to Phone System (No Codes)	✔	✔	✔	✔
» Two-way Intercom System With Call Buttons		✔	✔	✔
» Duress Button System - Office and Classroom		✔	✔	✔
» In-Building Emergency Communication System			✔	✔
» Distributed Antenna System (DAS)			✔	✔
» Mass Notification Tied to District-Wide System			✔	✔
» Building-Wide Communication via Outside Calls				✔
» Use of Mobile Applications and Social Media				✔

Tier Continuum — Layers — Components — Best Practices

INCREASING SECURITY →

Generally, each **best practice recommendation** presented in this guide corresponds to one of these components within a layer or across multiple layers. Best practice recommendations are further divided into **TIERS** along a "**TIER Continuum**" progressing from TIER 1, which provides a good baseline level of security, to TIER 4, which includes the most comprehensive approaches to securing a facility.

Many schools will not be able to implement TIER 4 measures and may not have a need to do so. The general purpose of this guide and its TIERS is to provide school administrators with tools they can use to gauge their risk levels, identify their security needs and, after factoring in available resources, develop security plans tailored to their schools or districts that incorporate practices and procedures vetted by experts.

Each TIER includes all recommendations in the preceding TIERS, and in many cases, implementation of best practices at the lower TIER level lays the groundwork for moving to higher levels of security in the long term. Whether officials at a school or district determine that implementing TIER 1 best practices would be best for their situation or identify risk factors that compel a move to other TIERS, this guide can help to inform and provide a rationale for decision making.

Recommended Uses

There are several specific ways the PASS Guidelines can be used to assist school administrators and other officials.

- **SUPPORT RISK ASSESSMENT AND DEVELOPMENT OF COMPREHENSIVE SECURITY PLANS.**
The Guidelines can be used by school officials, consultants and solutions providers to provide a common starting point for objective analysis and prioritization of school security needs. In this way, the Guidelines can be used as part of the risk assessment process or to define resulting recommendations (see Risk Assessment) or help initially formulate or update a comprehensive security plan to put recommendations into action.

  By identifying a given school or district's TIER levels, the Guidelines provide administrators with a frame of reference to communicate facility security status to school board members, parents and local officials as they seek support in advancing up the TIER Continuum as necessary to mitigate identified risk according to funding availability (see Appendix A for a step-by-step plan).

- **GRANT PROPOSAL DEVELOPMENT.** The federal government[6] and many states have provided significant funding for security improvements. The PASS Guidelines and best practices outlined here provide a framework for identifying the most critical needs and cost-effective solutions, information that can help strengthen and justify grant applications.

- **SCHOOL SAFETY/SECURITY STANDARDS.** Unlike with fire detection and suppression, building codes do not generally guide the implementation of security best practices as hard requirements. For the past 100 years, fire alarm systems have provided the communication mechanism used to alert students, staff and visitors to the presence of a fire threat inside a school. Fire alarms have long been required through adoption of NFPA 101, the life safety code, and NFPA 72, the fire alarm and signaling code, and as a result no students have lost their lives in a fire at a school since 1958.

  Proven best practices serve to guide efforts to set basic requirements for securing schools. Several states have established baseline standards or guidance for securing school facilities, often to augment state grant programs, and there are many states in which such policies are under consideration.[7] The PASS guidelines can help inform standards and guidance development efforts by policymakers or in the private sector.

- **AVOIDING PITFALLS.** Both administrators and providers benefit from being able to demonstrate effective use of technology and resources to meet specific security objectives, avoiding pitfalls that could result in the waste or underutilization of scarce resources in the pursuit of improved security.

  Not only can the information provided in the Guidelines help stakeholders stay informed on nationwide best practices, it also provides a reference point for evaluating specific solutions and products that are offered. *It is particularly important in today's climate that school officials be wary of aggressive marketing of any products that are unproven, inappropriate or even illegal for school use.*

---

[6] The U.S. Department of Justice School Violence Prevention Program, cops.usdoj.gov/default.asp?Item=2958.

[7] For more information on state school security programs, standards and funding, see the Secure Schools Alliance Research and Education website, secureschoolresources.org

PASS
Partner Alliance
for Safer Schools

TOP 10 K-12 SAFETY AND SECURITY PITFALLS:

1. Failure to assemble a planning team (see Policies and Procedures) that includes all appropriate and necessary stakeholders

2. Insufficient prioritization of security based on an "it won't happen here" mentality

3. Implementation of advanced technology and/or high-cost solutions without first ensuring baseline, proven security measures are in place (such as those found in TIER 1 in the PASS Guidelines)

4. Inconsistent implementation of disparate systems that do not meet security objectives identified in a comprehensive security plan or risk assessment

5. Short-sighted planning or products that respond only to the latest tragedy, as opposed to supporting a long-term, holistic approach

6. Choosing lowest-cost solutions above all other considerations, such as total life cycle costs

7. Reliance on technology for emergency communications that is not designed for such use

8. Overreliance on a single form of emergency communication or overdependence on a single type of solution or technology to address a broad range of safety and security challenges

9. Failure to appropriately balance external and internal risk mitigation—Based on risk assessment, different approaches may be more appropriate, depending on the facility. With active shooter events, for example, 100 percent of such incidents targeting elementary schools have been perpetrated by intruders from outside the school communities, while approximately 75 percent of incidents at secondary schools involved students or others associated with the schools.[8]

10. Unnecessary products that can be solutions in search of a problem. The recent proliferation of "barricade" or "secondary locking" devices is just one example. Offering no advantage over a modern lockset,[9] such devices are typically offered as a lowest-cost lockdown solution, in violation of fire and life safety codes and the Americans with Disabilities Act (ADA).
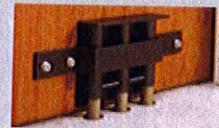
Example of "barricade" or "door blocker" devices

---

[8] Rural Trust Special Report on School Violence, 2013, ruraledu.org/articles.php?id=3082

[9] PASS Position Statement on Classroom Barricade Devices – www.passk12.org

Risk Assessment—A Prerequisite

Securing schools requires a risk mitigation mindset. What is risk? In everyday conversation, threat, vulnerability and risk are often used interchangeably to describe what we are trying to address with security; however, there are important distinctions between these terms.

- A threat is what we are trying to protect assets (people, property, etc.) against.

- A vulnerability is a gap in our protection efforts.

- A risk results where and when threats and vulnerabilities intersect.

Like any organization that invites people onto its property, schools have an obligation to provide a reasonable level of security to mitigate risks. In the commercial sector, this is viewed not as a reactive law enforcement function, but as a proactive security function.

A risk assessment is the first step toward developing a comprehensive security plan and thus a prerequisite for decisions regarding deployment of security solutions. Several options for conducting risks assessments are available through:

- Local police and fire officials (ability varies by jurisdiction)

- DHS protective security advisors[10]

- Independent consultants

- Security design consultants/systems integrators

- Internal assessment using free assessment tools

- Assessment by local subject matter experts assembled by districts

A building assessment of physical security at individual facilities is part of the risk assessment process, either for each district facility or for a smaller representative sample of facilities. Under the PASS Guidelines, TIER 1 best practices are basic security measures that should be implemented by all schools and districts, while higher-TIER practices should be guided by recommendations resulting from an assessment process. Many free assessments are available[11] and can provide a useful starting point for formulating a security plan especially when resources for assessments are limited. PASS also recommends using assessments provided by school safety centers in the many states where such centers have been established. Similar free resources are also provided by state governments[12] and the federal government. For building assessments, the NFPA 3000 Active Shooter and Hostile Event Response (ASHER) standard recommends the PASS Guidelines among other tools. See Annex A.5.4.2. of NFPA 3000 Chapter 5 (Risk Assessment).

---

[10] For more information, see dhs.gov/protective-security-advisors.

[11] Secureschoolresources.org/education-facilities-assessment

[12] As an example, see the Georgia Department of Education's School Safety Assessment, gadoe.org/Curriculum-Instruction-and-Assessment/Curriculum-and-Instruction/Documents/School%20Safety%20Assessment.pdf.

PASS
Partner Alliance
for Safer Schools

Risk assessments can cover a wide range of issues. Among these, there are many security-related threats facing schools in addition to other threats to safety, which is why a multifaceted, all-hazards approach is so important. These include but are not limited to:

- Theft

- Burglary

- Assault

- Sexual assault

- Kidnappers and sexual predators

- Workplace violence

- Active shooter/mass casualty attacks

- Homicide

- Suicide

- Gang activity

- Trespassing

- Bullying and harassment

- Parental custodial concerns

- Unsupervised visitors

- Vandalism/property destruction

- Compromise of confidential information

Risk assessment and mitigation can never eliminate risk; however, risks can be identified, measured and reduced. The best practices identified in the PASS Guidelines can be used for developing recommendations based on this process and formulating a plan to put them into action.

LAYERS OF PROTECTION

DISTRICT-WIDE

Leadership and coordination at the district level are integral to the successful development and adoption of school safety processes, plans, technologies and procedures and for ensuring these measures are updated for consistency with evolving best practices.

Most school safety measures have district-wide components or responsibilities. It is critical for districts to understand the fundamental link between readiness for day-to-day emergencies and disaster preparedness. School districts that are well prepared for individual emergencies involving students or staff members are more likely to be prepared for complex events like a community disaster or an active shooter incident. In the Guidelines, PASS outlines the components and best practices along the TIER Continuum at the district-wide level that schools and school districts can use in addressing a wide range of emergency situations that impact school safety, such as incidents of natural disasters, violence, mental health and medical emergencies.

PROPERTY PERIMETER

The property perimeter layer begins at the school property boundary and extends to the parking lot. This area includes playgrounds, sporting fields and other facilities that are often used by the public after school business hours end. The physical security of a school facility begins at the property perimeter, where the most outwardly visible security deterrents to an external threat can be implemented. The boundary should be clear to the public and provide visible notice of the rules and responsibilities for individuals entering school property.

PARKING LOT PERIMETER

Within the parking lot perimeter, staff, students and visitors park their vehicles or arrive and depart by bus or other means. Just like the property perimeter layer, the parking lot perimeter should always be clearly defined. In many cases, this area is where schools experience the most safety issues. Falls, car accidents, dangerous driving, theft, vandalism and assault are just some of the events that can take place in these areas.

BUILDING PERIMETER

The building perimeter layer begins with school grounds adjacent to the exterior structure of a building and consists of the perimeter of a building itself, including the exterior doors and windows of a school. Securing a building perimeter can range from simple to complex, especially for middle schools or high schools with multiple buildings/open campuses. Key safety and security functions take place within this layer, as it encompasses all areas where people enter and exit a school building.

CLASSROOM/INTERIOR PERIMETER

The classroom/interior perimeter layer consists of a school's entire interior, including not only classrooms but also gymnasiums, cafeterias, media centers, etc. This is both the last layer of defense against external threats and, often, the first protection against internal threats to student, staff and visitor safety.

PASS
Partner Alliance
for Safer Schools

SAFETY AND SECURITY COMPONENTS

POLICIES AND PROCEDURES

The 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. Essential security-specific policies and processes relevant to each layer are categorized under TIER 1 as foundational best practices.

PEOPLE (ROLES AND TRAINING)

Personnel (vigilant staff and students) make up the most important component of each layer. To individuals with criminal intent, such vigilance is an effective deterrent. ALL students and staff should be empowered to take effective action in emergencies and receive appropriate training and instructions relevant to a school or district's safety processes, plans, technologies and procedures.

ARCHITECTURAL

There are many architectural considerations that can enhance the security and safety plans for school buildings. Using Crime Prevention Through Environmental Design (CPTED) principles is critical to efforts by districts and their architects in designing buildings and grounds that enhance safety and security. Buildings should be designed to have natural surveillance (sight lines), territorial reinforcement (designated public, semi-private and private areas) and access control. The architectural component also includes collecting and sharing critical information about school facilities for mitigation and response to emergencies.

COMMUNICATION

Emergency communication is vital to the safety and security of the staff and students in our schools. It is important to distinguish between emergency and routine communication systems. An **emergency communication system** is defined by NFPA 72 (the national fire alarm and signaling code) as "a system for the protection of life by indicating the existence of an emergency situation and communicating information necessary to facilitate an appropriate response and action." **Routine communication systems** handle day-to-day communication on all matters outside this definition.

The use of dedicated emergency communication systems and technologies is essential. Normal business telephone, email and social media apps designed for routine communication are not adequate for critical communication during an emergency events unless they are specially configured for this purpose in a code-compliant manner. The 9/11 terrorist attacks and the 2011 tornado in Joplin, Missouri[13], are two of many examples in which these routine communication technologies failed during emergency situations.

---

[13] National Institute of Standards and Technology (NIST) Final Report, nvlpubs.nist.gov/nistpubs/NCSTAR/NIST.NCSTAR.3.pdf

ACCESS CONTROL

Controlling access to school property, buildings and classrooms is a basic security function and responsibility of school administrators. Mechanical locks have historically formed the base for any access control system, but there are other critical elements to consider. Many schools and districts have invested in electronic access control features that allow for enhanced security. Modern access control systems and procedures offer an effective solution to preventing unauthorized intruders from accessing a building during school hours and for monitoring access points for the various layers.

VIDEO SURVEILLANCE

A video surveillance system is a component of any school or district security program, providing deterrence and detection and, in more advanced implementations, enhancing response to a variety of daily challenges experienced at schools.

In the past, video recordings were used primarily in a forensic capacity to help determine the who, what, when and where of an incident after the fact. As surveillance technology has advanced, so have capabilities that allow security professionals to leverage video as a proactive tool to help mitigate risks before and as they occur. Much of this capability has been enabled through the widespread use and increasing affordability of internet protocol (IP) cameras over the past decade.

It is very important to note that, in video surveillance, there is no such thing as a "one-size-fits-all" approach. Designing a quality video surveillance system can be complicated and requires a collaborative approach involving multiple professionals.

DETECTION AND ALARMS

"Detection and alarms" refers to technology used to detect and/or report an emergency event. Traditional intrusion detection systems represent a key platform that has evolved beyond burglar alarms to provide the capability to report other types of emergencies and support an all-hazards approach to safety and security. The most important aspect of detection and alarm systems is that they provide the technological means to easily translate the detection of a security threat to a strategic notification that best fits with the processes and protocols put in place to respond to the threats that schools face.

Using the PASS Guidelines to Formulate a Comprehensive Security Plan

Here is a suggested roadmap for using the Guidelines to formulate a security management plan.

STEP 1—Assemble Team. Security planning teams should include key stakeholders in the K-12 environment. The process of forming a team should be led by an experienced security director, if a district is fortunate enough to have full-time staff in this position, or a staff member who has security as a primary responsibility. Start with a basic team including:

1. Security director

2. School administrator

3. Security/systems integrator and/or consultant

4. IT director

5. Local police and fire officials

In larger or more complex projects, it is also best to have a hardware consultant involved in the process.
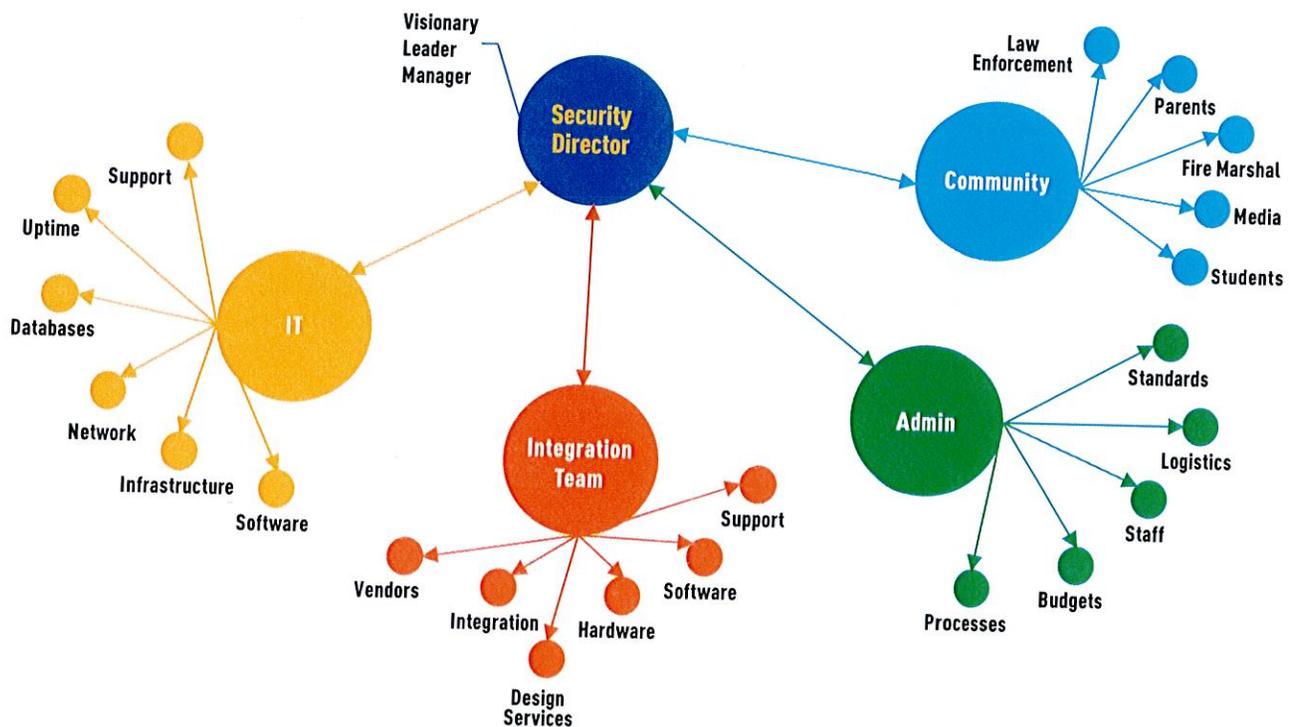
STEP 2—**Risk Assessment.** Most school buildings across a district have unique risk profiles. Complete a risk assessment for each building followed by a building assessment (using the PASS Guidelines Checklist), and develop the plan and budget for the building.

STEP 3—**Building Assessment Using Checklist by Layer**. The Building Assessment can be completed using the PASS Guidelines Checklist. Complete this process by reviewing each layer within the Guidelines. The district-wide layer needs only to be completed once, as it is designed to cover best practices that should be implemented across the entire district. For each individual building, complete the balance of the layers, including:

- Property Perimeter Layer

- Parking Lot Perimeter Layer

- Building Perimeter Layer

- Classroom/Interior Perimeter Layer

LAYER/COMPONENTS/BEST PRACTICES	TIER 1	TIER 2	TIER 3	TIER 4	Our Status			
					Achieved	In Progress	Future Need	Not Required
DISTRICT-WIDE								
• VIDEO SURVEILLANCE								
» Use and Data Retention Policy	✔	✔	✔	✔				
» MOUs with Law Enforcement for Sharing Video Data	✔	✔	✔	✔				
» Incorporation of Video Surveillance Into Emergency Response Plans	✔	✔	✔	✔				
» Camera Standardization		✔	✔	✔				
» Recording System Standardization			✔	✔				
» Video Verification of Alarms to Monitoring Service or Security Operations Center (SOC)				✔				

STEP 4—**Establish Documents and Budgets Based on Checklist Selections.** Security component and best practices descriptions found in the guidelines can be used to assemble a detailed document of the building/district plan. Budgets can be established using the estimated cost range for each best practice (online tool expected in 2019 at passk12.org).

DISTRICT-WIDE LAYER
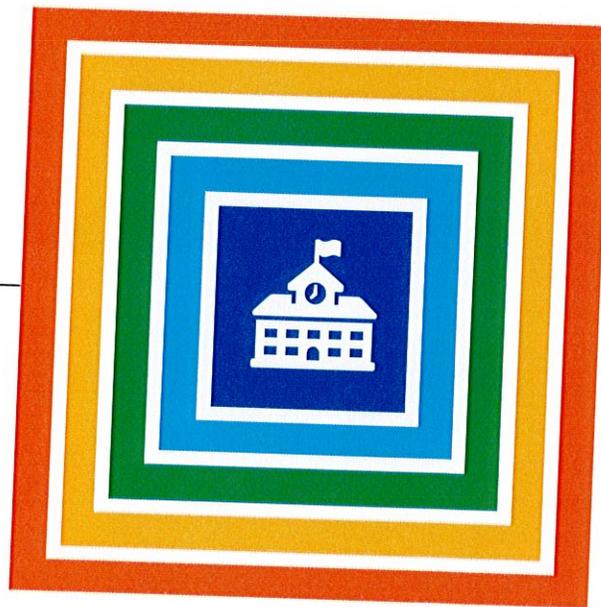
» QUICKFIND

DISTRICT-WIDE LAYER

• POLICIES AND PROCEDURES

	TIER 1	TIER 2	TIER 3	TIER 4
» School and District Emergency Protocols & Responsibilities Defined	✔	✔	✔	✔
» Dedicated Security Director/Department	✔	✔	✔	✔
» Climate and Cultural Survey of Stakeholders	✔	✔	✔	✔
» Establishment of Safety Policies and Procedures	✔	✔	✔	✔
» Sharing Maps and Other Facility Information With Law Enforcement, Fire and EMS	✔	✔	✔	✔
» District-Wide Physical Security Standards	✔	✔	✔	✔
» Annual Physical Security Assessments Based on District-Wide Standards	✔	✔	✔	✔
» Ensure Maintenance of Security Technology Implementations	✔	✔	✔	✔
» Incident Report Documentation System	✔	✔	✔	✔
» Independent Security Assessment on 5-Year Cycle				✔

VISITOR MANAGEMENT SYSTEM

	TIER 1	TIER 2	TIER 3	TIER 4
» Visitor Badging System	✔	✔	✔	✔
» Electronic Visitor Management System		✔	✔	✔

STUDENT AND STAFF IDENTIFICATION

	TIER 1	TIER 2	TIER 3	TIER 4
» Volunteer Background Checks	✔	✔	✔	✔
» Student Identification Badges	✔	✔	✔	✔
» Smart Card Identification Badges			✔	✔
» Biometrics-Based Authentication				✔

CYBERSECURITY AND NETWORK INFRASTRUCTURE

	TIER 1	TIER 2	TIER 3	TIER 4
» Segregate Physical Security Network From Administrative and Student Networks	✔	✔	✔	✔
» Optimize Power Over Ethernet Cabling Infrastructure to Support Security Devices	✔	✔	✔	✔
» MDF and IDF Frame for Servers, Connections and Head End Security Hardware	✔	✔	✔	✔
» Implement All Available Software and Firmware Updates	✔	✔	✔	✔
» Ensure Security Equipment Software and Firmware is Up to Date	✔	✔	✔	✔
» Incident Response and Redundancy Plan for Critical Security Systems	✔	✔	✔	✔
» Cybersecurity Best Practices Training	✔	✔	✔	✔
» Internal and External Penetration Testing		✔	✔	✔
» Automated Vulnerability Scanning		✔	✔	✔
» Compromise Assessment		✔	✔	✔
» Network Intrusion Detection			✔	✔
» Compromise Assessment			✔	✔
» Next-Generation Firewalls			✔	✔
» District-Wide Managed IT Network Cybersecurity Operations				✔

• PEOPLE (ROLES AND TRAINING)

	TIER 1	TIER 2	TIER 3	TIER 4
» Empower All Staff to Initiate Emergency Procedures	✔	✔	✔	✔
» Biannual All Hazard Scenario-Based Drills With Community Partners	✔	✔	✔	✔
» Empower Community to Share Concerns Through Anonymous Reporting	✔	✔	✔	✔
» Train All Staff and Volunteers on Mandated Reporting Requirements and Protocols	✔	✔	✔	✔
» First Responder Training for School Personnel Based on Local Needs	✔	✔	✔	✔

PASS
Partner Alliance for Safer Schools

	TIER 1	TIER 2	TIER 3	TIER 4
• ARCHITECTURAL				
» Facility and Vicinity Mapping	✔	✔	✔	✔
» Printed or Electronic "Tactical Floor Plans"		✔	✔	✔
» Building Information Modeling (BIM)			✔	✔
• COMMUNICATION				
» Memorandums of Understanding (MOUs) With Emergency Responders for Threat Information Sharing and Building Access	✔	✔	✔	✔
» MOUs With Hospitals, Religious Organizations, Community Centers and Red Cross	✔	✔	✔	✔
» Wide-Area Two-Way Radio System	✔	✔	✔	✔
» Trunked Radio System		✔	✔	✔
» Mass Notification Unified With Emergency Communications System			✔	✔
WEATHER MONITORING				
» Monitor NOAA Local Weather Information	✔	✔	✔	✔
» Weather Monitoring Service		✔	✔	✔
» Weather Monitoring Station at Central School Facility			✔	✔
» Weather Monitoring Station at School Facilities Every 10 Miles				✔
• ACCESS CONTROL				
» Command Staff/Responder Access to Keys or Credentials for Emergency Entry	✔	✔	✔	✔
» Access Control System Equipped With Remote Door Release Capability			✔	✔
» All Command Staff Possess Keys and/or Access Credentials			✔	✔
» All Responders Possess Keys and/or Access Credentials				✔
» Electronic Access Control for IDF & MDF Rooms w/Key Override				✔
AUXILIARY BUILDINGS				
» Implement Security Plan Specific to Auxiliary Buildings	✔	✔	✔	✔
TRANSPORTATION				
» Interoperable Radio System for All Buses and School Vehicles	✔	✔	✔	✔
» GPS Tracking System for All Student Transportation Vehicles	✔	✔	✔	✔
» Bus Video Surveillance System		✔	✔	✔
» Card-Based Check-In				✔
» Biometric-Based Check-In				✔
• VIDEO SURVEILLANCE				
» Use and Data Retention Policy	✔	✔	✔	✔
» MOUs with Law Enforcement for Sharing Video Data	✔	✔	✔	✔
» Incorporation of Video Surveillance Into Emergency Response Plans	✔	✔	✔	✔
» Camera Standardization		✔	✔	✔
» Recording System Standardization			✔	✔
» Video Verification of Alarms to Monitoring Service or Security Operations Center (SOC)				
• DETECTION AND ALARMS				
» Intrusion Detection System for All Buildings Centrally Monitored	✔	✔	✔	✔
» Duress Alarms Centrally Monitored	✔	✔	✔	✔
» Duress Alarms Sent to Law Enforcement		✔	✔	✔
» Duress Alarms Monitored by a District-Wide SOC			✔	✔
» Intrusion and Duress Alarms Monitored by a District-Wide SOC				✔

PASS Partner Alliance for Safer Schools

POLICIES AND PROCEDURES COMPONENT:

Two national response models serve as the framework for local policies, procedures and response plans. For larger-scale emergencies and disasters, the National Response Framework (NRF)[14] offers guiding principles that enable all response partners to prepare for and provide a unified response to disasters and emergencies—from the smallest incident to the largest catastrophe. The term "response" (as defined by NRF) includes taking immediate action to save lives, protect property and the environment and meet basic human needs. Response also includes the execution of emergency plans and actions to support short-term recovery. The NRF also describes how agencies, such as schools, can work together with communities, tribes, states, the federal government and private partners.

Secondly, the National Incident Management System (NIMS)[15] is a comprehensive national design for conducting incident management. NIMS provides the template, while the NRF provides the structure and mechanisms for incident management. A key component of NIMS is the Incident Command System (ICS),[16] which provides a standardized approach for incident management, regardless of cause, size, location or complexity. By using ICS during incidents, schools and districts will be able to more effectively work with the responders in their communities.

To maximize success, effective management of school emergencies requires training, preparation and planning. Schools are responsible for anticipating and preparing to respond to a variety of emergencies. The policies and procedures outlined below will help empower the students and staff to respond in an emergency, closely aligned with the phases of emergency management:

Prevention/Mitigation: Staff should be given the training and opportunity through a continuous process to identify actions addressing hazards from all possible sources and to reduce the potential for an emergency to occur. Examples could include educating students and staff about recognizing and reporting suspicious behaviors and persons and addressing gaps in measures to control access to school facilities.

Preparedness: Districts should develop community-wide security and emergency preparedness planning groups, using the ICS framework. This includes establishing standard emergency response plans and practicing skills, drills and other exercises to evaluate both the response capabilities of a school and the effectiveness of their all-hazards planning. Staff and students should be prepared to recognize and respond to emergency situations with options for appropriate action.

Response: School employees should understand their roles and expectations in responding to an emergency, both during and after the emergency. Additionally, students can be taught different skills for dealing with an emergency.

Recovery: Following a disaster, a district has a responsibility to parents and school personnel to provide direct support and serve as the liaison between community resources and those in need, including both short- and long-term recovery; this responsibility can include monitoring and responding to student and staff health status and mental health and psychological response.

---

[14] fema.gov/plan

[15] fema.gov/national-incident-management-system

[16] fema.gov/incident-command-system-resources

TIER 1

A. School and District Emergency Roles & Responsibilities Defined. Each school district should formally adopt through board policy the NRF and NIMS developed by the Federal Emergency Management Agency (FEMA). When adopting NRF and NIMS, a school district should implement an ICS within the entire organization as the coordinating link between multiple agencies and jurisdictions in an emergency response. Each district should adopt ICS as the management structure to be used in school and district EOPs[17], ensuring that plans developed include any elements that are required by state law.

NIMS uses a core set of concepts, principles, procedures, processes, standards and terminology that should be integrated with school emergency management practices. The collective use of NIMS across all local incident response agencies, including K-12 schools, creates a common operating picture and, ultimately, more efficient and effective response. Furthermore, in the event of a large-scale incident crossing multiple jurisdictions and disciplines, NIMS unites all response teams across all participating jurisdictions and facilitates and draws assistance from outlying communities when needed based on the size and complexity of the incident.

At a minimum, key district personnel should complete these NIMS trainings:

- Safety Team Members & Backups—ICS 100SCa[18]
- District Crisis Plan Developers—ICS 100SCa and IS 362[19]

A prerequisite for developing EOPs and setting other security related policies and procedures is the creation of collaborative planning teams. Operational planning is best performed by teams and ideally led by full-time district safety and security directors (see below). Planning teams should include representatives from a wide range of school personnel, including, but not limited to, administrators, educators, students, parents, school psychologists, nurses, facilities managers, transportation managers, food personnel and family services representatives. Teams should also include student and parent representatives and individuals and organizations that serve and represent the interests of students, staff and parents with disabilities, others with access and functional needs and racial minorities and religious organizations so that specific concerns are included in the early stages of planning.

A planning team should be small enough to permit close collaboration with first responders and other community partners, yet large enough to be representative of the school and its families, community and culture.[20] The team should also be large enough as to not place an undue burden on any single person. Examples of the types of teams that can be created include:

- District crisis response team (ICS)
- Building crisis response team (ICS)
- District safety planning team
- Building safety planning team
- Multi-agency crisis planning team (can be combined with the district safety planning team)
- Threat assessment team
- Psychological recovery team

---

[17] training.fema.gov/programs/emischool/el361toolkit/assets/sampleplan.pdf

[18] training.fema.gov/is/courseoverview.aspx?code=is-100.sca

[19] training.fema.gov/is/courseoverview.aspx?code=is-362.a

[20] For suggested members of a security team, see Safe and Sound Schools toolkits, safeandsoundschools.org/programs-2/toolkits/

In addition, planning teams should include community partners, such as responders, local emergency management staff and others who may have roles and responsibilities in school emergency management before, during and after an incident. Community partners include local police and fire officials, emergency medical services (EMS) personnel, school resource officers (SROs), fire officials, public and mental health practitioners and local emergency managers. Their expertise will inform the development, implementation and refinement of EOPs.

Importantly, EOPs should detail the role of safety and security technology during an emergency, requiring operational proficiency among staff in leveraging these tools. Such technology can provide situational awareness, audit trails and vital information for first responders. Under the ICS model, plans should also ensure there are backup personnel trained and ready to properly use technology as well.

B. **Dedicated Security Director/Department.** Districts should designate a security director tasked with district-wide security management duties and responsible for the effective implementation of security policies and programs. Ideally this should be a full-time position with additional staff if needed as part of a security department; however, for many districts, staff tasked with security management will also perform additional functions.

C. **Climate and Cultural Survey of Stakeholders.** Conducting an anonymous climate and cultural survey allows a school district to obtain valuable information on the views of students, staff and parents that can inform planning teams on safety and security issues.

A climate and cultural survey should measure the following:

Safety

- Rules and Norms: clearly communicated rules about physical violence; clearly communicated rules about verbal abuse, harassment and teasing; clear and consistent enforcement and norms for adult intervention
- Sense of Physical Security: sense that students and adults feel safe from physical harm in the school
- Sense of Social/Emotional Security: sense that students feel safe from verbal abuse, teasing and exclusion

Teaching and Learning

- Support for Learning: use of supportive teaching practices, such as encouragement and constructive feedback; varied opportunities to demonstrate knowledge and skills; support for risk taking and independent thinking; atmosphere conducive to dialog and questioning; academic challenge; and individual attention
- Social and Civic Learning: support for the development of social and civic knowledge, skills and dispositions, including effective listening, conflict resolution, self-reflection and emotional regulation, empathy, personal responsibility and ethical decision making

Interpersonal Relationships

- Respect for Diversity: mutual respect for individual differences (e.g., gender, race, culture) at all levels of the school— student-student, adult-student, adult-adult and overall norms for tolerance.
- Social Support—Adults: pattern of supportive and caring adult relationships for students, including high expectations for students' success, willingness to listen to students and get to know them as individuals and personal concern for students' problems
- Social Support—Students: pattern of supportive peer relationships for students, including friendships for socializing, problems, academic help and new students

Institutional Environment

- School Connectedness/Engagement: positive identification with the school and norms for broad participation in school life for students, staff and families
- Physical Surroundings: cleanliness, order and appeal of facilities and adequate resources and materials

For Staff Only

- Leadership: administration creates and communicates a clear vision and is accessible to and supportive of school staff and staff development
- Professional Relationships: positive attitudes and relationships among school staff that support effectively working and learning together

D. **Establishment of Safety Policies and Procedures.** Each district should ensure that, within the policies and procedures established for staff and students, parents, volunteers and any others that interact with the school community, the following are covered:

- School safety/NIMS compliance
- All-hazards procedures
- Staff safety training
- Threat assessment
- Discipline
- Harassment and bullying
- Use of technology
- School engagement and truancy
- Pandemic procedures
- Food allergies and handling procedures
- Mail handling procedures
- Drug and alcohol prevention
- Student safety training
- Staff assignments for supervision of students within layers (see below)
- Violence prevention, awareness and reporting procedures
- Suicide prevention, response and reporting
- Mental health issues (e.g., depression)
- Child abuse
- Violence prevention, awareness and reporting procedures
- Plans and procedures for students, staff and community members with disabilities

E. **Sharing Maps and Other Facility Information With Law Enforcement, Fire and EMS.** One of the most important lessons learned from school-based emergencies is the importance of having basic maps and other information ready for use by responders in emergencies. Information such as facility maps, aerial photos and building access information (see Architectural Component) should be provided to local police, fire and other emergency responders. As schools present unique challenges to emergency responders due to size, complexity and occupants, responders require extensive amounts of detailed yet easily understandable information in the event of an attack or other emergency at a school.

The type and format of information shared should align with the inspection and pre-incident site planning processes commonly used by fire departments and HAZMAT personnel to gather, analyze and store a broad range of data. Such data includes but is not limited to mechanical system shutoffs, evacuation routes, on-site hazards, camera locations, card access points, mass notification devices, intercoms and other information in a standardized format. Under these processes, pre-planning is also divided between a tactical "quick action" overview of a site and a strategic plan that provides more in-depth and detailed information about a site. This dual approach is useful because the information required during the initial minutes of a response may differ from that needed for longer, more strategic responses.

F. **District-Wide Physical Security Standards.** Managing physical security resources includes strategic planning, identifying goals and performance objectives and justifying and applying a realistic budget. Every school district should establish and implement security standards for its facilities to guide this process. The PASS Guidelines provide a resource that may be used in the development of such standards and the prioritization of related security initiatives.

G. **Annual Physical Security Assessments Based on District-Wide Standards.** A proper school security assessment examines five safety areas: safety, security, climate, culture and emergency preparedness.

- Safety—the risk associated with the most common and most serious school safety incidents, such as parking lot and playground injuries and fatalities
- Security—an evaluation of access control, visitor management, video surveillance, locks, security policies and other approaches to reduce risks associated with the risk of school violence and other types of criminal activity
- Climate—assessing the perceptions of those within the school community
- Culture—the values and behavioral norms of students, parents and staff that relate to the other safety areas
- Emergency Preparedness—a thorough and holistic evaluation of emergency response preparedness provides the best opportunity to prevent death and serious injury once a crisis occurs

H. **Ensure Maintenance of Security Technology Implementations.** The implementation of security and life safety technology creates a district-wide responsibility to ensure this equipment is always properly maintained and operational; this is commonly accomplished through carrying out a program of periodic testing, either by staff or through built-in monitoring features or third-party monitoring services that can warn staff when electronic equipment is not functioning properly. One of the best ways to address equipment failures is to ensure that installation agreements provide for timely equipment replacement when necessary. Additionally, some school districts (especially larger districts) employ security technicians who can troubleshoot and repair problems immediately. It is important to note that many security equipment manufactures offer training and certifications that technicians working with this equipment should obtain.

I. **Incident Report Documentation System.** To improve mitigation efforts and responses to future events, school districts should thoroughly document all safety- and security-related events or policy violations that take place within the district, no matter how minor; this documentation can be accomplished by assigning a staff member to document and maintain records of all incidents for the district. This system can be as simple as maintaining a basic electronic spreadsheet or using professional report documentation software. Incident data should be categorized as specifically as possible to better enable the most useful analysis possible, which can be used to educate stakeholders about factors influencing security operations.

TIER 4

A. **Independent Security Assessment on 5-Year Cycle.** Third-party assessments help school districts identify potential vulnerabilities and strengths relating to security and safety for students, staff and visitors. An evaluator should have considerable documented experience in conducting security and safety assessments for school systems.

Assessments should take a holistic look at a district's safety and security posture and include the following areas:

- Effectiveness of policies, plans and procedures
- Visitor screening procedures
- Use of CPTED
- Access points
- Analysis of surrounding neighborhoods
- Anti-terrorism measures
- Liability reduction opportunities
- Access control (building perimeter and interior)
- Video surveillance systems
- Alarm systems
- Student supervision
- School climate
- Bullying abatement strategies

VISITOR MANAGEMENT SYSTEM:

TIER 1

A. **Visitor Badging System**. Every school should have a visitor badging system. While these systems can range from basic to advanced, at a minimum visitor badges should be issued to all individuals visiting schools who are not staff or students. A school should sign all visitors in to a log using the visitors' government-issued identification cards and checking the student information system to ensure 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)

TIER 2

A. **Electronic Visitor Management System**. Visitor management systems are technology solutions that streamline the visitor sign-in process and track specific visitor data such as who is entering the school and when, the reason for the visit and who was visited. Additionally, many systems record photos of the visitors or scan driver's licenses that are presented by visitors not only to help confirm the identity of the presenter, but also to check for persons that should not be permitted to enter for a variety of reasons, such as restraining orders or parental rights disputes. Some systems check driver's license data against the National Sex Offender Database or even run full criminal background checks. Most solutions also have built-in volunteer tracking capabilities that allow school districts to track their hours, which is helpful to those that use these hours for property tax rebates and other purposes. Most systems also have built-in badging services.

STUDENT AND STAFF IDENTIFICATION:

TIER 1

A. **Volunteer Background Checks**. Volunteers play an increasingly important role in the school community by providing many hours of their time to mentor, coach and tutor students and additionally supplement staff in many ways; however, volunteers also present a security vulnerability that many districts have struggled to address, requiring a balance between properly screening out unqualified individuals and encouraging participation from dedicated, privacy-conscious volunteers. School districts should screen volunteers to verify their identities and identify any potential problems, especially problems that could arise from an undisclosed criminal history. Some states require or facilitate school volunteer background checks, while others have no established screening requirements.

Laws that require volunteer screening generally specify only that the individual undergo a criminal history check or a criminal history check plus a check of sex offender registries. Each school district should draft a policy regarding volunteers and what type of background check they should obtain. Failure to maintain trust can be devastating to an organization and lead to loss of community support, loss of funding or even a lawsuit for negligent selection of a volunteer. Even when faced with an incident involving a volunteer, a district will fare better by having made a good faith effort to conduct a background check before the incident occurred.

B. **Student Identification Badges**. Providing student identification badges (in secondary schools) supports increased safety and security in several ways. Being able to determine whether a person is a student enrolled at the school and is supposed to be inside a school at a given time is extremely important to the safety and well-being of all students and staff. Identification badges are simple and secure ways to easily determine who is supposed to be on campus if they are required to be worn visibly and presented to school staff upon request; this can be especially important to responders during emergency events, as they are not likely to be familiar with the students.

TIER 3

A. **Smart Card Identification Badges.** In more advanced implementations, smart cards with radio frequency identification (RFID) or near field communication (NFC) technology allow students and/or staff to check in electronically to the building, classrooms, buses and any other place where there is a need for documentation and accountability and provide a mechanism for secure payment in cafeterias. Since smart cards are coded with an electronic profile that is assigned to card owner, additional functionality, including use across access control systems, can easily be added when necessary. In a phased implementation, school districts can start with a basic ID system and add other features later when budgets allow or needs change.

TIER 4

A. Biometric-Based Authentication. Biometrics deployments in K-12 schools will become more mainstream as the technology is widely deployed in the private sector to streamline business practices and secure financial transactions. While the primary rationale for use of biometrics by a school or district is to enhance such administrative functions, there are security-enhancing applications as well. Using biometrics like fingerprints and facial recognition can verify or identify an individual rather than a credential (like cards or keys). For example, biometrics readers can be implemented for access control purposes, eliminating the need for (and expense of) using cards, which can be lost, stolen or damaged, or the need for verifying students have been safely picked up/dropped off safely (see discussion under Transportation).

Educating all stakeholders, including parents when student use is involved, is critical to the success of any biometrics implementation in the K-12 setting. Providing clarity and transparency about how the technology works can help address any misperceptions about the use of information collected or potential for misuse. Properly implemented, use of biometrics serves to enhance, versus compromise, identity security.

Fingerprint technology offers a good example of how biometrics authentication technology can enhance safety and operations without compromising privacy. During electronic enrollment of the biometric, a student's fingerprint is translated to a numerical abstraction based on features of the finger lines, creating a unique code that is then associated with a student's identity in the school's database. The fingerprint itself is not recorded—only the unique code issued by the server for the lines of the fingerprint is retained. From a technological standpoint, the process cannot be reversed to create a fingerprint based on the unique code. Additionally, all biometrics providers use proprietary algorithms to create and read the code, making it even more difficult for the information to be misused. In any case, use of biometrics should be governed by a use policy set at the district level, include requirements such as providing an opt-out procedure to ensure participation is voluntary and ensure the destruction of all biometric-related information associated with a student or employee when they end their association with a school.

CYBERSECURITY AND NETWORK INFRASTRUCTURE:

There are two primary types of cybersecurity risks that can interfere with a school district's safety and security objectives and its ability to respond to emergencies:

1. **Cybercrime Against the School Community Enabled by Compromise of Sensitive or Personal Information.** School districts manage enormous amount of data within their enterprises, including personal identity information, health records, financial information, Social Security numbers for students and staff and critical academic records. There are several important federal requirements for managing and securing this data, including the Family Educational Rights and Privacy Act, the Health Insurance Portability and Accountability Act and the Fair Credit Reporting Act. Many public schools still use legacy IT infrastructures (or partial migrations) and must work with tight budgets that limit their ability to upgrade to newer technology that is less vulnerable to threats. These challenges are exacerbated by the requirement to support open data exchange in the interest of education, along with school-issued or personal laptops, tablets and smartphones that may connect to a school's network. All these factors make school districts a prime target for cybercrime.

2. **Compromise of Physical Security Systems via Cyberattack or Failure of Network Infrastructure.** IT infrastructure that is not protected, designed or configured correctly could provide an opportunity for attackers to compromise safety and security systems. Similarly, unpatched software or firmware, defective code, open permissions and misconfigurations of connected physical security systems (access control, video surveillance, alarms, etc.) also presents possible cyber vulnerabilities that could be exploited by attackers to gain access to other connected systems and data on the network.

The following are specific best practice recommendations for identifying, segregating and controlling access to the physical security system and protecting sensitive information; however, the **Cybersecurity Framework**[21] developed by NIST, part of the U.S. Department of Commerce, should be the starting point for all cybersecurity efforts. The framework includes cybersecurity standards specifically for protecting our nation's critical infrastructure, which includes education facilities.

TIER 1

A. **Segregate Physical Security Networks From Administrative and Student Networks**. Security and emergency communications systems (access control, video surveillance, alarms, etc.) should be operating on dedicated physical security networks (subnets and/or VLANs), separate from the districts' primary operational networks and any student networks, with proper security controls in place; this not only provides better cyber protection for physical security systems, but it also preserves operation of these critical systems if operational networks fail for any other reason. IT and physical security staff should meet on a regular basis to discuss the latest challenges and industry trends—to keep in front of the threats as much as possible. If a district has a dedicated physical security department or a dedicated individual employee for this function, it is recommended that this department create internal service-level agreements with the IT department to perform IT tasks related to security equipment or security-related network infrastructure.

---

[21] nist.gov/cyberframework.

B. **Optimize Power Over Ethernet Cabling Infrastructure to Support Security Devices.** Broadband high-speed internet and related networking infrastructure have provided tremendous benefits for schools, enhancing classroom instruction and other capabilities while also enabling connected security devices. Virtually all security solutions depend at least in part on physical network infrastructure, the most important of which is power over ethernet (POE) cabling. Public schools can use federal E-rate program funding[22] for POE infrastructure, helping to offset and lower the total cost of security investments.

POE infrastructure should be developed and managed to support security systems and functions. Security devices should be segregated from both administrative and learning services connections. Color-coding POE cabling is one way to achieve this that makes wire identification and locating devices easier (e.g., blue cabling=video, green cabling=access control, purple cabling=learning services).

C. **Main Distribution Frame (MDF) and Intermediate Distribution Frame (IDF) for Servers, Connections and Head End Security Hardware.** MDF and IDF rooms are used to store, organize and secure servers and connections and head-end security hardware. MDF and IDF rooms should be climate controlled and protected with intrusion alarms and electronic access control that logs and stores access data (see Access Control).

D. **Implement All Available System Software Patches and Vulnerability Remediation.** School districts are responsible for ensuring all software system patches and vulnerability remediation occur on schedule, unless there is a specific contract in place with a service provider to do so. Many software and hardware suppliers provide cybersecurity vulnerability notifications. Remediation may include patching (patches should be tested on a subsystem before enterprise-wide installation to ensure compatibility) and workarounds (the quick fix that may involve shutting off vulnerable features and functions, before a patch is available from the supplier). Updates to mitigate cyber vulnerabilities should also include upgrading to the latest operating systems for PCs. The use of modern operating systems such as Windows 10 automatically means using the latest malware and anti-virus tools.

E. **Ensure Security Equipment Software and Firmware Is Up to Date.** It is particularly important for security and IT staff to work together to ensure security systems and networked devices are running the latest firmware versions and any available patches are correctly installed to protect against potential cyber vulnerabilities.

F. **Incident Response and Redundancy Plan for Critical Security Systems.** Every school district needs a cybersecurity incident response plan. When staff know what processes to follow, there is a greater chance the impact of a cybersecurity incident can be minimized. Such plans should include redundancies to ensure critical security systems remain operational and all systems are backed up daily.

G. **Cybersecurity Best Practices Training.** Schools and districts should offer periodic training to staff on how to guard against cyberthreats in routine practice. Criminals are using automated tools, social engineering (trust-based emails that make you click on a bad link), malware, phishing, spear phishing, ransomware and other methods that could disable a network just as easily as a targeted hacking attack. It is also a growing and valuable practice for IT departments to perform their own controlled and managed email scams to see if staff respond as per procedure, strengthening the "human firewall."

---

[22] For more information, fcc.gov/general/universal-service-program-schools-and-libraries-e-rate.

PASS
Partner Alliance for Safer Schools

TIER 2

A. **Automated Vulnerability Scanning.** School districts can use commercially available vulnerability scanning tools to regularly test the system for known vulnerabilities and report potential exposures. Vulnerabilities typically include unpatched or misconfigured systems.

B. **Internal and External Penetration Testing.** District IT departments can conduct periodic network penetration exercises to determine if there are any weaknesses in the network that could be exploited. If possible, an independent verification and validation (IV&V) external penetration test should be performed.

TIER 3

A. **Network Intrusion Detection.** Intrusion detection monitoring services and software examine traffic on the network or activity on host computers to provide real-time notification and/or interception of cyberattacks.

B. **Compromise Assessment.** Conducting a periodic compromise assessment determines to what extent, if any, a system has already been compromised by looking for evidence of hackers or malicious software, the exfiltration of data, reconnaissance and other signs that remediation is required.

C. **Next-Generation Firewalls.** "Third" generation firewall technology provides advanced security features such as intrusion prevention, network traffic filtering, encrypted traffic inspection and bandwidth management, which limit the spread of compromised systems and malware if attacked.

TIER 4

A. **District-Wide Managed IT Network Cybersecurity Operations.** A credible managed service provider can carry out many of the functions described above under one umbrella, including:

- Device management and security monitoring in real time
- Managed endpoint security
- Host- and network-based intrusion detection and prevention services
- Managed firewall and managed web app firewall
- Real-time malware detections system
- Incident response/plans and preparedness
- Digital forensics
- Penetration testing from a third-party service provider
- Web and mobile app tests
- Compromise assessment tools

PEOPLE (ROLES AND TRAINING) COMPONENT:

TIER 1

A. Empower All Staff to Initiate Emergency Procedures. School districts should empower each staff member with decision-making authority, means and training on options-based solutions to take needed actions in emergencies. For example, all school staff should be able to initiate lockdowns when appropriate. During an active threat incident where there is a danger of grievous bodily harm or threat to occupants of a school, staff need to know how to reduce their risk and protect lives until help arrives.

They need to know:

- What to do in the emergency
- How to make independent decisions and act on them immediately
- What strategies and options they can use
- When and where to do it
- Who is responsible for what, and their individual roles
- How to communicate with others responding to the emergency

There are often no universal all-encompassing plans to cover threat response. Differences in the school campuses and the school population will influence what kind of response plan is right for each school district.

At a minimum, protocols that employees should be trained to independently initiate are:

- **Lockdown.** A lockdown usually involves locking and closing doors, moving students out of sight and requiring students to remain quiet within the room. Lockdowns should continue to be included in any an options-based approach to active assailant training, which provide students and staff with a range of alternative strategies to save lives and the permission to use them, considering variables such as the nature of the threat, time of day and location of students. Like other safety drills (e.g., fire or tornado), it is important that the ages and developmental levels of students and the physical layout of the school campus (e.g., ease of access to outside doors and proximity of places to hide other than classrooms) are considered when communicating to students and staff concerning lockdown.

- **Secured Perimeter (Lockout).** A secured perimeter addresses threats outside the building, often initiated when there are emergency situations taking place in neighborhoods nearby, such as a crime in progress, police activity or a dangerous animal in the area.

- **Shelter in Place.** Shelter in place is initiated in situations that may require staff and students to shelter in their classrooms or work areas; it is more restrictive than a secured perimeter, as staff and students are not allowed to move within the building. Unlike in a lockdown, however, staff and students can remain at desks or work spaces. Shelter in place is generally initiated when there is a possibility that an area emergency may escalate and having students and staff sheltered behind locked doors may be critical to safety and order.

- **Evacuation.** The purpose of an evacuation is to quickly get students and staff out of the building by a route designed to avoid contact with a potential threat, generally avoiding the location of a known threat inside the building, such as a suspicious package, a threatening person in a specific confined area or a hazardous material spill.

- **Reverse Evacuation.** A reverse evacuation procedure is used to get students and staff into the safety of a building to avoid contact with a potential threat when the location of the threat outside the building is known.

- **Room Clear.** A room clear procedure is initiated by a teacher or supervising adult to send students away from a potential threat, such as a student acting out in a violent manner; it is also used when the teacher must remain in the dangerous situation but can send students to a designated safe area.

Teachers and supervising staff have several important responsibilities before, during and after an emergency, as students will rely upon them first for direction. The actions of teachers and supervising staff are critical to helping the incident command team and others respond appropriately to the emergency at hand. Staff must follow the directives of the site administrator/ principal or their designee and carry out directives in a swift, organized and calm manner that conveys confidence to students.

Staff should do the following before an emergency:

- Know the school's incident command response procedures.
- Keep an updated paper copy of the class roster readily accessible—not on a computer.
- Pre-position emergency supplies such as water, food and first aid items that may be necessary during an extended confinement.
- Prepare activities or simple games to occupy children during an extended confinement.
- Prepare students for emergency response by instructing students and practicing drills as directed by the site administrator.

During an Emergency:

- Carry out all the site administrator's directives.
- Get students' attention and be a calm, efficient leader.
- Direct students to evacuate or shelter in place as indicated.
- Take attendance and account for all students.
- Assist disabled students.
- Remain with students at all times.
- Report missing or injured students to the site administrator/principal or their designee.
- Restore order and assist other staff as necessary.
- Reassure and occupy students with an activity as appropriate.
- If not on duty, report to the site administrator.
- Document all activities that occur during the emergency.

Students should be taught to understand the types of threats that may be encountered on campus. They should learn **option-based** strategies for how to respond to an active threat both inside and outside the school. These strategies should include appropriate response options for each situation, such as shelter, evade and defend.

Additional emergency protocols for which all staff, teachers and substitutes should be trained:

Weather and Natural Caused Emergency Procedures:

- Severe weather conditions
- Hurricane
- Thunderstorm and lightning

- Tornado
- Flash flood warning
- Earthquake
- Air quality index

Immediate Danger Emergency Procedures:

- Dangerous/suspicious person on campus
- Hostage situation
- Suicide threat or attempt
- Lost or missing child
- Kidnapping/abduction
- Student or staff death/medical emergency
- Assault/sexual assault
- Weapon on campus

Fire, Terrorism, Hazardous Material and Utility Loss Emergency Procedures:

- Fire or explosion
- Hazardous material spill
- Biohazard
- Utility loss
- Body fluid precautions
- Act of terrorism—nuclear/biological/chemical weapon
- Bomb threat procedure

Miscellaneous Emergencies

- Nearby emergency
- Civil disturbance
- School bus for field trip emergency
- Crime scene/crime in progress
- Angry visitors
- Rules of giving descriptions
- Animals on school grounds
- Unmanned aerial vehicles

B. **Biannual, All-Hazard, Scenario-Based Drills With Community Partners.** A "tabletop" exercise is a table-based activity typically held in an informal setting and presented by a facilitator. There is no hands-on practice or field work. This type of exercise is intended to generate discussion of various issues regarding a hypothetical, simulated emergency. Tabletops can be used to enhance general awareness, validate plans and procedures, rehearse concepts and/or assess the types of systems needed to guide the prevention of, protection from, mitigation of, response to and recovery from a defined incident. Another great solution for training is to create tabletop drills with multiple scenarios. The drill topics should be realistic and foster an understanding of incident command and your district's capabilities.

Delivered in a low-stress environment, a tabletop exercise offers participants the opportunity to explore different ideas in the context of a real-world scenario. All participants should be encouraged to contribute to the discussion and reminded that they are making decisions in a "no-fault" environment. Effective facilitation is critical to keeping participants focused on exercise objectives. The facilitator may ask about the decisions made, including how a decision was reached or what implications a decision might have. It is also helpful to conduct annual tabletop drills that include a district's community partners such as police, fire and Red Cross.

Another good practice is to open school facilities after hours for training by police and fire personnel. In addition to providing an ideal space for training, this will allow these officials to familiarize themselves with district facilities.

C. **Empower Community to Share Concerns Through Anonymous Reporting.** Use of communications tools allowing students and others in the community to anonymously report potential threats and other concerns has demonstrated success in preventing potential violence. Students often know long before adults do what is occurring in their schools and communities— including fighting and bullying, substance abuse, dangerous and concerning behaviors, threats, depressions, suicide and self-injury, witnessed either in person or online. Some states, such as Colorado, mandate public schools to implement tip line programs.[23]

Tip reporting processes should be simple; provide students, parents and community members with a safe way to report information about any issues that concern their safety or the safety of others; and meet the following criteria:

- The anonymity of every report should be guaranteed—no caller ID or data tracking.
- The program should be available to all members of the community.
- Calls should be answered immediately, and service should be available 24 hours a day, every day of the week.
- Every tip should be investigated.

D. **Train All Staff and Volunteers on Mandated Reporting Requirements and Procedures.** All states have laws requiring individuals serving in specific capacities to report suspected child abuse to an appropriate agency, such as child protective services or a law enforcement agency. Teachers, principals and all other school personnel are mandatory reporters. The circumstances under which a mandatory reporter must make a report vary from state to state. Typically, a report must be made when the reporter, in his or her official capacity, suspects or has reason to believe that a child has been abused or neglected. It is important for school districts to create training, policy and awareness concerning this responsibility.

E. **First Responder Training for School Personnel Based on Local Needs.** School employees in school-based emergencies are the very first responders and should be provided with basic training in first aid protocols, including CPR and use of automatic external defibrillators at a minimum. The American Red Cross is the largest provider of training is this area and also offers a free evaluation tool called the Ready Rating program.[24] Another popular course for school employees is the Community Emergency Response Team program offered by DHS,[25] which includes basic instruction on the principles of search and rescue and firefighting. Many other first responder training programs are available that are relevant to trauma, mental health and other needs in tragedies.

---

[23] Safe2Tell Colorado, safe2tell.org/?q=safe2tell-colorado-mobile-app.

[24] Readyrating.org.

[25] Ready.gov/community-emergency-response-team.

ARCHITECTURAL COMPONENT:

TIER 1

A. **Facility and Vicinity Mapping.** As noted within the Policies and Procedures component, schools present unique challenges to emergency responders due to their size, complexity and occupants. Responders require extensive amounts of detailed, 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:

- Printed or electronic copy of "As-Built/Record Drawing" of the subject facility. Plans should include all room names and associated numbers (see discussion of door and window numbering systems under the building perimeter layer).

- Printed or electronic copy of an aerial view of the subject facility. This should include a minimum five-block radius outside the school property perimeter.

TIER 2

A. **Printed or Electronic Tactical Floor Plans.** In addition to as-built/record drawings of the subject facility, "tactical floor plans" include basic room name/numbers and identification of security cameras and other access control devices.

TIER 3

A. **Building Information Modeling (BIM).** BIM provides a digital, three-dimensional representation of a facility that allows users to virtually "walk through" the environment while accessing information about its features and toggling between a range of display views from "tactical" to "comprehensive strategic" features.

COMMUNICATION COMPONENT:

TIER 1

A. **Memorandums of Understanding (MOUs) With Emergency Responders for Threat Information Sharing and Building Access.** Information sharing is an important form of communication, and a provides the primary template for and means of two-way information sharing and coordination between organizations and individuals from different organizations. MOUs should be established with local police, fire and EMS in two primary areas relating to emergency communication.

- **Threat Information Sharing**—Districts should provide information to responders regarding how they can use school communications systems to communicate that a threat is imminent, whether it is a security or non-security threat or a weather emergency, etc., and vice versa. For example, a weather emergency could affect one or more schools within the district. A MOU should detail how communication can be initiated to the school(s) and/or district in a quick and efficient manner.[26]
- **Emergency Building Access**—Districts should provide information to emergency responders regarding the security and life safety elements of the building and of systems inside the building (see Facility and Vicinity Mapping under the Architectural Component). Clearly defining where individuals should and should not routinely access the school building assists in adding a layer of security. Since all school buildings must have a certain number of doors that lead out of the building in case of a threat inside the building, it is important to note which doors are for emergency egress only and which are used to enter the building.

B. **MOUs With Hospitals, Religious Organizations, Community Centers and Red Cross.** EOPs typically incorporate participation by local facilities and organizations for evacuation, trauma care, mass casualty response, family reunification, mental health recovery and other purposes if needed. These relationships with community organizations should be governed by MOUs so that roles and responsibilities are clearly defined and all parties can be adequately prepared to act if needed.

C. **Wide-Area Two-Way Radio System.** From a district-wide perspective, a two-way radio communication system is recommended to quickly and efficiently communicate threats to the district or to certain schools within the district. A wide area network radio system allows reliable voice communications with key district staff who would be the first to respond in an emergency. The system should allow for all administrators, principals, security personnel and transportation staff to have two-way radios. Since public schools are government entities, commercial radio systems licensed under the Federal Communications Commission (FCC) Universal Licensing System[27] must be used, not off-the-shelf consumer products or radios designed for recreational use.

TIER 2

A. **Trunked Radio System.** A trunked radio system allows organization of users into different groups and provides the capability to communicate on frequencies used by police, fire, EMS and other first responders in the community, whereas traditional two-way radio systems may be confined to a certain band (frequency) exclusive to the system.

TIER 3

A. **Mass Notification Unified With Emergency Communications System.** On a district level, mass notification systems that are installed in each school should have the ability to be networked so that the district can use the mass notification system to provide district-wide communication to school facilities. There are several technologies currently available that allow for the individual communication systems to be unified.

---

[26] Example of a MOU on radio communications with local law enforcement - arapahoegov.com/AgendaCenter/ViewFile/Item/5368?fileID=7523

[27] For license example, see wireless2.fcc.gov/UlsApp/ApplicationSearch/applMain.jsp?applID=9075468.

WEATHER MONITORING:

The most likely risk a school may face on any given day is a weather emergency. In their emergency preparedness protocols, school districts should practice for the types of weather emergencies that they may face.

TIER 1

A. **Monitor National Oceanic and Atmospheric Administration (NOAA) Local Weather Information**. One of the simplest means for weather monitoring is for each school to monitor the local NOAA weather feed[28] for their community and use a NOAA weather radio. A school district should ensure adequate pre-incident planning in monitoring the upcoming weather conditions to prepare for emergencies.

TIER 2

A. **Weather Monitoring Service.** Subscription-based services are available that provide specialized weather monitoring such as site-specific weather notifications as well as access to 24-hour meteorological consultation. This can play an important role in areas prone to weather dangers such as lighting and tornados. Site-specific warning technology typically includes lighting proximity and all-clear notifications that can help protect students and staff participation in outdoor events.

TIER 3

A. **Weather Monitoring Station at a Central School Facility**. The most effective way for a school district to address weather emergencies is to install a weather monitoring station at a centralized school facility location; this provides the most accurate information on the actual weather conditions in an area and helps ensure actions taken are not based on inaccurate or incomplete information from other sources. Weather stations also benefit education programs by providing classes with access to weather data. The community can benefit in other ways as well, through incentives offered by the private sector to school districts to install weather stations at schools. This data is shared with and used by the community through various weather monitoring smartphone apps, including apps that provide information on live weather conditions and the threat from severe weather events such as lightning, hail, strong winds, heavy snow, hurricanes, flooding and other weather conditions that would impact school safety.

TIER 4

A. **Weather Monitoring Stations at School Facilities Every 10 Miles.** Multiple weather stations may be required to achieve the same in-house functionality for a district that spans large geographic areas, with recommended placement every 10 miles for the most site-specific accuracy.

---

[28] noaa.gov/weather.

ACCESS CONTROL COMPONENT:

Controlling access to school buildings is fundamental to securing the school environment. Access control can consist of both mechanical and electronic systems. **Mechanical systems** are locking devices with mechanical keys, and **electronic systems** consist of electronically controlled locking mechanisms, card readers and cards.

A limited number of key operated openings should be provided to allow access to different areas of a building from the exterior in the event alternate access to the building is required. Electronic access control is a preferred approach, as electronics allow control of who can access specific openings at specific times.

TIER 1

A. **Command Staff/Responder Access to Keys or Credentials for Emergency Entry.** Mechanical keys should be available to district and community emergency responders for all mechanically or electronically controlled openings to provide an emergency override. Preferably, this should be a master or grand master key to access both exterior and interior doors. Such keys should not be widely distributed. They must be carefully controlled and limited to key personnel and emergency responders.

TIER 3

A. **Access Control System Equipped With Remote Door Release Capability.** This capability allows remote opening of any door that is part of an electronic access control system from a central station to allow entry by law enforcement or other responders.

B. **All Command Staff Possess Keys and/or Access Credentials.**

TIER 4

A. **All Responders Possess Keys and/or Access Credentials.**

B. **Electronic Access Control for MDF and IDF Rooms With Key Override.** MDF and IDF rooms house and protect district network infrastructure (see Cybersecurity and Network Infrastructure).

AUXILIARY BUILDINGS:

A. **Implement Security Plan Specific to Auxiliary Buildings.** Physical protection systems are just as necessary at school district auxiliary buildings as they are at main instructional buildings. Auxiliary buildings are transportation centers, educational centers, warehouses and other places in a school district that are not considered instructional facilities. Auxiliary building security should not be neglected and should be addressed with the same measures deployed in schools to protect facilities and occupants. Security infrastructure for auxiliary buildings should be unified with a district's overall physical security systems and procedures. Resource allocation should be based upon risk analysis, maximizing use of current deployed security technology and coordination of security efforts within the district and with community partners.

PASS
Partner Alliance
for Safer Schools

TRANSPORTATION:

On any given day in America, millions of students ride school buses to and from school. Many of the same security technologies that have been deployed in schools are now deployed on buses. One of the most important practices is the deployment of advanced communications equipment that goes beyond traditional radio use. Bus communications platforms provide digital radio communications, GPS tracking, student accounting, text and email communications, engine diagnostics, driver behavior analysis and other data. Fully using these capabilities also provides the opportunity for school districts to streamline transportation costs.

TIER 1

A. **Interoperable Radio System for All Buses and School Vehicles**. All buses and other school vehicles should be equipped with interoperable radio systems, connecting administration, principals, teachers, security, maintenance, bus drivers, coaches and law enforcement agencies. By equipping staff and bus fleets with two-way radios and bridging software, schools can communicate directly with other responders when an emergency occurs. Whether providing care to an injured student, reporting weather conditions or situational information, this information can be shared instantly with responding agencies and other school personnel. To achieve radio interoperability, a district must coordinate with other community stakeholders, including local law enforcement agencies. Throughout the country most jurisdictions use the same two-way radio communication systems that allow users sharing the same range of frequency to communicate with the others in emergencies (trunked systems).

B. **GPS Tracking System for All Student Transportation Vehicles.** GPS is a satellite-based technology that provides both real-time and historical location data recording. GPS tracking can allow a school district to know where buses and school vehicles are in real time and allow integration with a card-based or biometrics check-in system. GPS tracking systems can be configured to record the location of the device at regular intervals (data loggers), report location and other vehicle data wirelessly in real time (data pushers) or allow users to remotely request and retrieve such information (data pullers), generally when connectivity or power is available intermittently and real-time data is not required.

TIER 2

A. **Bus Video Surveillance System.** School bus surveillance systems provide an increasing number of safety and security benefits. Increases in both capability and affordability has led many districts to implement this technology. A typical school bus camera system consists of two to eight specialized mobile cameras, components and a mobile digital video recorder for each vehicle. Camera systems can both monitor the inside of the vehicle, including driver/operator behaviors during routes, and record the external environment through outward-facing cameras. In addition to video data, the system can record signals from the vehicle, including braking, right and left turning, warning lights and stop-arm deployment; it can also record sensor events such as vehicle speed, alarms and idle time. Sensors can be integrated into the system that measure any amount of force that was exerted on the vehicle during the route. For example, if the driver took a hard turn, or if there was a collision with another vehicle, the force of movement would be measured by the sensor, which can trigger an alarm event that can be quickly retrieved from the video. Importantly, school bus cameras can also capture student and driver behaviors, which could be vitally important in the review of an incident by school officials. As noted, school bus video surveillance systems can be integrated with GPS, RFID and biometrics for other related safety and security purpose.

TIER 4

A. **Card-Based Check-In.** School districts can deploy smart ID card systems to increase bus rider accountability and security. Such cards are embedded with microchips that use RFID technology or NFC to log when and where a student boards and exits the bus. This information allows school officials to know whether students were on the right buses and if they got off on the right stops. These cards can also be used to alert parents of where their child's bus is and when their child has entered or exited the bus.

B. **Biometric-Based Check-In.** Biometrics are the measurement and analysis of physical and behavioral characteristics unique to an individual, and biometrics technology provides an accurate way to authenticate identity that may be more efficient and secure than other methods. Biometric-based check-in is used for the same purposes as card-based check-in but may offer a more reliable process without the need for the student to remember and carry an ID card. Any use of biometrics in K-12 schools should be carefully tailored to the school setting, based only on proven physiological identifiers. Fingerprint/finger geometry is the most common, followed by facial recognition technology and others. Educating all stakeholders, including parents, is critical to the success of any biometrics implementation of biometric-based check-in.

VIDEO SURVEILLANCE COMPONENT:

Video surveillance is an integral component of a school's physical security plan; it provides deterrence, detection and, in more advanced implementations, enhanced response to a variety of daily challenges experienced at schools.

Video surveillance uses include:

- **Surveillance**—Monitoring video in real time, either manually or though an automated process
- **Assessment**—Viewing recorded video to assess a situation that is currently happening or recently happened
- **Forensics**—Using recorded video data to provide a record of what actually happened during an event, including use as evidence of unlawful or impermissible activity
- **Risk Mitigation**—Using video analytics to proactively notify security or other personnel that an event is taking place

For decades, video recordings have been used in a forensic capacity to help determine the who, what, when and where of an incident after the fact. As surveillance technology has advanced, so have the capabilities enabling security professionals to leverage video as a proactive tool that helps mitigate risks even as events unfold. Much of this capability has been enabled through the widespread use and increasing affordability of IP cameras over the past decade. Harnessing these advances aligns with a tiered approach. While some analog video systems are still in use, it is recommended that new installations for K-12 be specified with IP cameras as a fully networked system. Existing analog systems should be updated as funds become available, as the nature of video surveillance technology allows for updating functionality over time without replacing earlier investments.

Management of video surveillance assets and use policy at the district level will help ensure the most effective use of the technology to support safety and security across facilities and the most efficient use of resources.

TIER 1

A. **Use and Data Retention Policy.** A video surveillance use policy and a data retention policy should be defined at the district level to ensure consistency across all schools. The purpose of a video surveillance use policy is to document and provide clear instructions as to how video surveillance will be used in daily operations, while a data retention policy defines how long recorded video will be retained. From a liability perspective, both documents will demonstrate "reasonable" efforts by the district to define and follow these policies in the event of legal action. Some states have produced guidelines and standards for school security that may address video data, so it is important to refer to them in your policy if applicable.

A **video surveillance use policy** should define:

- Who has authority to actively view cameras live during school hours and afterwards (Surveillance, Assessment).
- When video data can be used to support disciplinary actions (Assessment, Forensics).
- When and how video will be shared externally, such as with parents or law enforcement (Forensics).
- How recorded video of identified incidents, particularly events involving potential unlawful or impermissible activity, will be handled and stored. For example, whether incident recordings will be stored on separate media devices and kept longer than the defined retention policy for non-incident data (Forensics).
- How, if applicable, video analytics will be used (Risk Mitigation).

A **video surveillance data retention policy** should define:

- The number of images per second or frame rate that the system will be recording at—if different cameras are recording by varied frame rates, such as by location or use of analytics, then it should be clearly defined in the policy.
- Number of days recorded video will be retained during and immediately following the school year.
- Number of days recorded video of specific incidents, including incidents that resulted in a disciplinary response, will be retained.

B. **MOUs With Law Enforcement for Sharing Video Data.** MOUs should be established between the district and local law enforcement if schools intend to share recorded or live video of incidents. The ability to stream video directly to law enforcement provides valuable situational awareness during emergencies but may not be desired during normal daily operations. This is a decision that needs to be made at the district level and documented appropriately. Such MOUs document who decides when video will be shared and under what circumstances. This should be a collaborative effort with law enforcement and other community stakeholders. The MOU should also ensure training is provided to law enforcement to become familiar with the operation of your video management system (VMS) so that they can operate it independently when needed.

C. **Incorporation of Video Surveillance Into Emergency Response Plans.** Use of video surveillance to provide remote situational awareness during incidents should be incorporated into emergency response plans. Valuable information can be relayed to law enforcement responders who are en route to or, in the case of EMS, waiting to enter a facility. Law enforcement may use video surveillance to determine the threat level of a given area. For example, under the NFPA 3000 standard for responding to active shooter events, control zones are established that define the threat level of an area and the personnel or competencies that are needed to operate in that area. Defined as hot, warm and cold, assignment of these areas is the responsibility of law enforcement. Information from the video surveillance system may provide key information necessary for making this determination, which could mean the difference between EMS entering an area or not.

The plan should also document who is responsible for operating the video surveillance system during an emergency and how they will communicate with law enforcement. In many cases, law enforcement may have access to the video directly or may request access to the video surveillance on site. In either case, schools should still assign someone to this role so that they can assist law enforcement if needed. This person should be trained in the use of the system and included in emergency drills and have a backup in case that person is not on site or incapacitated.

TIER 2

A. **Camera Standardization.** Equipment standardization provides better life cycle management options and shortens downtime when devices fail or are damaged. At the district level, schools should consider standardizing on specific camera models based on intended use, such as "hallway cameras," "parking lot pan-tilt-zoom (PTZ)" or "Entrance/Exit Cameras." This does not necessarily mean standardizing on one manufacturer's products district-wide; rather, it means making consistent decisions on devices that meet operational requirements for given types of locations. It is not uncommon to have equipment produced by multiple manufacturers recording to the same VMS, but by limiting the number of different models installed, districts can keep on hand spare equipment that can be rapidly deployed if needed.

TIER 3

A. Recording System Standardization. Standardizing video surveillance recording devices should be considered to provide a consistent user interface and experience across all schools in the district; this will decrease operational training costs by having only one system with which security personnel need to be proficient. Standardization enables the assignment of backup personnel for staff across different schools in the district to be integrated into emergency response plans; it also provides better life cycle management options for the district.

Most importantly, standardizing on a specific VMS provides a district with the ability for a centralized security operations center (SOC) to help manage video surveillance at schools throughout the district. Many districts have multiple recording platforms that have been deployed over the years at different schools. If the upfront cost to bring these systems under one platform is prohibitive, a planned migration can be established that defines the decision criteria for bringing schools into the new system as budgets allow.

TIER 4

A. Video Verification of Alarms to Monitoring Service or SOC. Many schools use intrusion detection systems that are monitored by offsite, central station companies that will dispatch law enforcement, EMS, fire or district security personnel based on the nature of the alarm. To reduce false alarms, some locations require alarms to be "verified" before these first responders can be called or dispatched. In the past, this typically meant calling or sending someone to the site of the alarm to verify the alarm. Today, video verification capability provides central station monitoring services with the ability to verify alarms remotely in cases where there is camera coverage of the affected space.

Another option for a school district is to develop their own SOC that replaces the need to hire a third-party organization to monitor alarms. There are staffing, capital and ongoing operational costs associated with this approach to be considered.

DETECTION AND ALARMS COMPONENT:

Detection and alarm systems use sensors or devices that are generally either hardwired or wireless or a combination of both. A hardwired system uses devices (e.g., door position switches, latch bolt monitors, motions sensors, glass break detectors) that are physically wired to a control panel that sends an alert to a central monitoring facility. Monitoring can be done via a telephone line, a broadband connection or cellular communications or a combination of these. A wireless system uses similar devices; however, the devices are battery powered and use radio signals to communicate to the control panel rather than a wire. Alerts are transmitted via the same communication mechanisms provided for the hardwired design.

The advantage of a wireless system is the ability to place a sensor or communications device in any location, including a device that staff can carry on their persons. The disadvantage is that radio signals can be affected by the building structure and additional radio communications infrastructure may be required to ensure signals can be transmitted and received from all areas of a school.

Districts should consider both designs when examining the implementation of intrusion detection and duress alarm systems. The type of design (hardwired vs. wireless) and monitoring (centralized vs. decentralized) should be based on the risk assessment and specific MOU established with first responders.

Another important aspect of detection and alarm systems is their ability to be configured as "decentralized" (standalone) or "centralized" (unified) systems. A decentralized system is specific to an individual property and reports alarm events separately, while a centralized system can monitor multiple buildings, alerts and technologies as one unified system. School and district officials should work with local law enforcement and first responders to determine the best system type to use for a facility or facilities. A centralized system allows for advanced features like immediate notification to first responders via two-radio and mobile- and PC-based technologies, while decentralized systems typically rely on a third-party central monitoring station to provide the alerts and notifications to first responders.

TIER 1

A. **Intrusion Detection System for All Buildings Centrally Monitored**. Intrusion detection provides a significant barrier against threats through deterrence. From a district-wide standpoint, intrusion detection systems are used to mitigate threats to facilities when unoccupied. Preventing unauthorized access to school buildings after hours helps mitigate common threats such as vandalism and theft, but intrusion detection also plays a broader security role, as such access could also enable a range of more serious safety and security concerns.

Securing the building through intrusion detection can be as simple as monitoring each exterior doorway through door position sensors and latch bolt sensors that are monitored by a central source. The central source can be a monitoring service, such as one that monitors for fire detection, local law enforcement emergency operation centers or a district security operations center.

From a district perspective, all school buildings should be monitored for whether an exterior door or window is breached while the building is unoccupied. The technology used to accomplish this can incorporate hardwired or wireless solutions that are readily available.

B. **Duress Alarms Centrally Monitored.** Intrusion detection systems and emergency communication and fire detection systems allow for an easy expansion of duress (panic) buttons or similar technology to the system. These duress buttons can be used for active threats, weather emergencies, medical emergencies and other security threats. Like intrusion detection, duress alarms should be monitored by a central source.

TIER 2

A. **Duress Alarms Sent to Law Enforcement.** Once an intrusion detection system is in place, it is important to define certain types of security threats that should be immediately sent to local law enforcement. Traditionally, an intrusion detection system transmits a possible threat to a centrally monitored station. That threat is classified by the central monitoring organization, and then appropriate first responders are notified of the threat. Duress alarms, however, should ideally be sent immediately both to appropriate district staff and to local law enforcement under a MOU governing this process.

The vast majority of situations in which a duress alarm is triggered will not be an active shooter event. It would be prudent, however, for a district to create a MOU with local law enforcement agencies that all duress alarms should be responded to as though the threat is a worst-case scenario. Not only does this response ensure that local law enforcement is notified of a threat immediately; it also allows for the accumulation of data to better understand what threats are facing schools in the district and the effectiveness of the policies, procedures and technology involved.
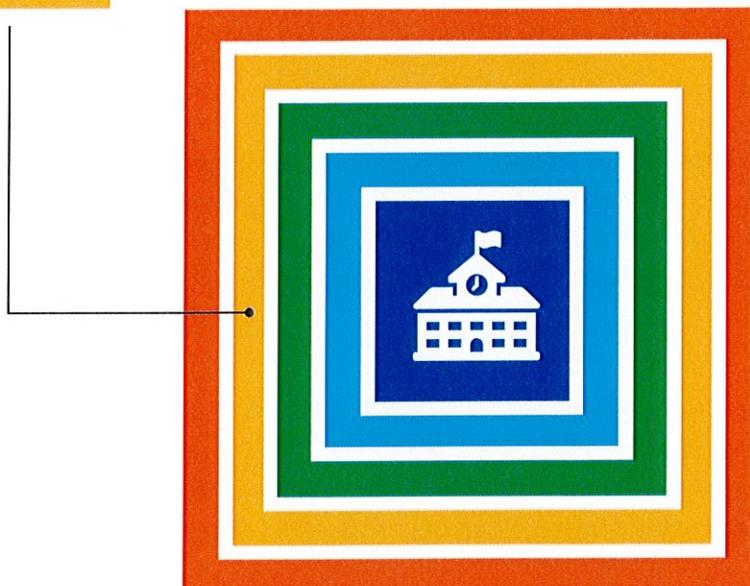
TIER 3

A. **Duress Alarms Monitored by a District-Wide SOC.** For districts that can implement a SOC, all duress alarms should be monitored and responded to by district security personnel. The advantage of having a SOC is that a district can use the technology to further enhance the all-hazards approach, as it can be configured to allow for alarm communications to the SOC for a wider variety of events than those where fire, EMS or law enforcement response would be required.

TIER 4

B. **Intrusion and Duress Alarms Monitored by a District-Wide SOC.** District security personnel that know the facilities, students and staff are in the best position to quickly determine the nature and appropriate response to alarms, managing other security systems and emergency communications from a centralized location. Intrusion and duress alarms monitored by a district SOC is the most desirable implementation because it adds a holistic layer to augment local responders.

PROPERTY PERIMETER LAYER

» QUICKFIND

PASS
Partner Alliance
for Safer Schools

PROPERTY PERIMETER LAYER	TIER 1	TIER 2	TIER 3	TIER 4
• POLICIES AND PROCEDURES				
» Implement NCS4 Best Practices for Outdoor Activities and Events	✔	✔	✔	✔
» Security Patrols		✔	✔	✔
» Annual Assessment for Lighting			✔	✔
• ARCHITECTURAL				
» Signage Directing Visitors to a Designated Entrance	✔	✔	✔	✔
» Apply CPTED Principles to Promote Territorial Reinforcement	✔	✔	✔	✔
» Trespassing, Video Surveillance and Access Notification Signage	✔	✔	✔	✔
» Properly Positioned Exterior Lights	✔	✔	✔	✔
» Debris Clearance	✔	✔	✔	✔
» Gates at Entrances	✔	✔	✔	✔
» Landscaping to Control Vehicle Access		✔	✔	✔
» Lighting to Enhance Video Surveillance		✔	✔	✔
• COMMUNICATION				
» Audible Mass Notification for Students and Staff	✔	✔	✔	✔
» Local Area Two-Way Radio System Between Office and Staff		✔	✔	✔
» Visual Indicators Specific to Hazard			✔	✔
» Digital Low-Band Radio System Connected to District-Wide System			✔	✔
» Audible and Visual Mass Notification Tied to District-Wide System				✔
• ACCESS CONTROL				
» Manual Access Gates		✔	✔	✔
» Electronic Access Gates				✔
• VIDEO SURVEILLANCE				
» Fixed Camera, Wide Area Coverage	✔	✔	✔	✔
» Wide Dynamic Range Cameras	✔	✔	✔	✔
» Infrared (IR) Cameras or Lighting		✔	✔	✔
» Wireless Video Data Transmission		✔	✔	✔
» PTZ Camera Coverage		✔	✔	✔
» Loitering Detection Analytics		✔	✔	✔
» Perimeter Video Analytics				✔
» People Identification at Gates or Points of Entry				✔

POLICIES AND PROCEDURES COMPONENT:

TIER 1

A. **Implement National Center for Spectator Sports Safety and Security (NCS4) Best Practices Guide for Outdoor Activities and Events.** PASS recommends that school districts use the best practices guide[29] developed by the NCS4 when developing policies and procedures for outdoor activities and events. To promote a consistent methodology for security planning for interscholastic sporting events and after-school activities, the NCS4 has established an annual National Interscholastic Athletics and After-School Activities Safety and Security Summit to bring together representatives from various public and private high school athletic administrations, school resource officers (SROs) and public safety agencies to address current safety and security issues facing interscholastic athletics and after-school events.

Additionally, school employees and volunteers should be trained to immediately question anyone on school property, even at the furthest perimeter point, who does not have a visitor's pass and is not accompanied by a school official. It is important, however, for school employees to have communication devices such as a school radio or cell phone to use to notify the office or others that they are about to make contact.

TIER 2

A. **Security Patrols.** School districts can assign security patrols and/or encourage law enforcement to have patrolling officers to discourage trespassing and other unwanted activities.

TIER 3

A. **Annual Assessment for Lighting**. A safety and security assessment of lighting based upon industry and local standards should be performed annually.

---

[29] NCS4, *Interscholastic Athletics and After-School Safety & Security Best Practices Guide, 2018 Edition*. For more information, see ncs4.com/knowledgeportal/best-practices.

ARCHITECTURAL COMPONENT:

TIER 1

A. **Signage Directing Visitors to a Designated Entrance.**

B. **Apply CPTED Principles to Promote Territorial Reinforcement.** Using CPTED promotes "territorial reinforcement" by clearly designating school property. Fencing, plantings, berms or a blend of all three can be used to discourage trespassers, well meaning or otherwise.

C. **Trespassing, Video Surveillance and Access Notification Signage.** In addition to the physical cues noted above, signage along the boundary of school grounds sends an unambiguous message regarding the hours (if any) when the public is welcome.

The property perimeter should be clearly defined with signage stating that entry onto school property is limited to authorized visitors and those on official school business. In cases where school grounds are used by the public after school hours, however, signage at these schools should include hours the grounds are open to public and what activities and items are prohibited, such as drug or alcohol use, unleashed pets, fireworks, dangerous horseplay and weapons. If your district has a security or law enforcement department that monitors and responds to situations on school property, it is recommended the department phone number be posted on the signs. Signage to discourage illegal dumping should be posted on dumpsters and in immediate areas.

D. **Properly Positioned Exterior Lights.** Outdoor lights should be installed at strategic points on the property perimeter and illuminate the area evenly during periods of darkness so that unauthorized and criminal activities are more easily recognized. Lighting should be directed toward the area rather than outward, with fixtures employing cut-off shrouds which limit "hotspots" for security cameras (either current or future), eliminate glare for residential neighbors and preserve night sky.

E. **Debris Clearance.** The school property should be clear of debris. Trees, shrubs and other growth should be cut back to minimize interference with lines of sight throughout the property. Annual inspection should be scheduled to maintain clear sight lines and limit places where individuals could hide for criminal purposes.

TIER 2

A. **Gates at Entrances.** Gates should be installed at all drive entrances or at other strategic drive "choke points" to allow school officials to effectively lock down the perimeter after regular business hours. This practice discourages the use of school property for unauthorized and/or illegal activities.

B. **Landscaping to Control Vehicle Access.** Materials such as decorative rocks, shrubs and planters to help keep vehicles off unauthorized areas of property.

TIER 3

A. **Lighting to Enhance Video Surveillance.** Outdoor lighting should be implemented specifically to enhance video surveillance visualization. Strive for relatively consistent foot candle[30] levels across the area to be monitored, as even lighting allows better imaging than uneven lighting. Minimum foot candle illumination set forth by local planning and zoning authorities generally supports effective lighting levels for surveillance video monitoring.

---

[30] A "foot candle" is the most common unit of measure used by lighting professionals to calculate light levels in businesses and outdoor spaces. A foot candle is defined as the illuminance of a single candle within a one-foot radius.

COMMUNICATION COMPONENT:

TIER 1

A. **Audible Mass Notification for Students and Staff.** Schools should ensure the ability to provide one-way communication to the green space areas of the school property. Green space areas include:

- Areas between school buildings in which students and staff are present during class changes
- Playgrounds and athletic fields within the property perimeter
- Reunification points within the property perimeter

The minimum standard of providing critical communication outside of the school building is to ensure that students and staff who are not within the building receive a clear, concise and easy-to-understand audible message. This notification can be performed through various low-voltage systems. Mass notification capability within the property layer could be achieved through the addition of a zone on the emergency paging system or fire alarm system that has the voice component.

TIER 2

A. **Local Area Two-Way Radio System Between Office and Staff.** The property layer of a school encompasses anything from playgrounds to athletic fields. To enhance the ability to communicate a threat to students and staff, a two-way radio system allows the administrative staff to communicate immediately with staff who are responsible for the students who may be outside of the building.

TIER 3

A. **Visual Indicators Specific to Hazard.** Providing more than one form of communication (audible) during an emergency event is preferred. The use of visual indicators outside of the building allows for the students and staff to be made aware 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.

B. **Digital Low-Band Radio System Connected to District-Wide System.** As discussed above, a two-way radio system is the most efficient way to quickly communicate with staff and students outside of the building. A district can implement a two-way radio system that also communicates on a district- and community-wide level. Within the property perimeter, this allows the staff outside the school to communicate to the district and local emergency responders as needed by simply changing the frequency on the radio.

TIER 4

A. **Audible and Visual Mass Notification Tied to District-Wide System.** Many intercom, emergency paging and fire alarm voice communication systems include the capability to be networked into one district-wide system. This technology allows for the use of products from multiple manufacturers integrated together to provide a unified system. Districts should explore using existing technology already installed in schools to economize and maximize the ability to provide a district-wide emergency communication system.

ACCESS CONTROL COMPONENT:

Access control may or may not be required at the property perimeter depending on risks specific to the geographic location of the property and where the access point(s) is located. As appropriate, and after an assessment determines it is necessary to do so, gates can be left open during school drop-off and pickup times. Note—in some locations, particularly urban settings, access gates will need to be placed within the parking lot perimeter due to space constraints.

TIER 2

A. **Manual Access Gates.** Manual gates to control access to the property must be physically unlocked and opened by staff at the beginning of open hours and likewise physically closed at the end.

TIER 4

B. **Electronic Access Gates.** Electronic gates can be installed at each entry point, including features such as intercom voice communication to the front office for vehicle entry and card access for staff and authorized visitors.

VIDEO SURVEILLANCE COMPONENT:

The perimeter of a school includes the area immediately surrounding the facility and school property where students and staff congregate for activities. It may include athletic fields, playgrounds, parking lots and other general use areas. In many cases, school property borders commercial or residential zoned areas. It is not uncommon for access to school property to be restricted during school hours but open to the public during off hours and the weekend. The differences in location and multi-use nature of school property means that no two schools are alike. A proper risk assessment will define the risks and mitigation techniques that should be employed.

Video surveillance is one component that can be used to mitigate risks for school perimeters by providing **surveillance, assessment, forensics and risk mitigation** as defined in the district-wide layer in the Guidelines.

Today, there are many different capability levels available in video surveillance equipment. Establishing an "operational requirement" for each camera deployed ensures the selection of equipment appropriate to the specific uses for which it is intended. These operational requirements are generally defined as:

- **Detection**—The ability to determine whether a person or object is in the field of view of the camera

- **Recognition**—The ability to differentiate and classify people and objects in the field of view of the camera (e.g., man or woman, child or adult, red or blue jacket, two cars and one truck)

- **Identification**—The ability to identify specific individuals or objects where present in the field of view of the camera (e.g., John Smith, a 2009 Toyota Camry, a license plate number)

Each of these operational requirements is defined by the number of "pixels on target" recorded of the object or person in the field of view. For people, the number of pixels measured across the width of their face determines what operational requirement is achieved. While there are no established standards to define pixels on target to meet specific operational requirements, the following chart outlines generally accepted thresholds in the security industry.

Operational Requirement	Horizontal Pixels/Face	Pixels per Inch
Identification	80	13
Recognition	20	4
Detection	4	1

Unless otherwise determined in a risk assessment, **recognition** and/or **detection** are the operational requirements for video surveillance of large outdoor areas.

TIER 1

A. Fixed Cameras, Wide Area Coverage. Fixed cameras provide video surveillance of outdoor activities taking place in the cameras field of view. Cameras should be rated for outdoor use to prevent ingress of dust or water and environmentally rated to function in both upper and lower temperature ranges.

The field of view should overlap the desired coverage area by at least one meter (when applicable) to ensure that the surveillance, assessment and forensics use cases are met. In some cases, cameras can be mounted directly on the building that houses the system's recording devices; this is the most cost-effective approach but can limit the field of view. Other mounting options include adding cameras to new or existing lighting poles around the property perimeter or on other buildings on the school property such as athletic or maintenance structures. All these mounting options present the challenge of transmitting the video data back to the facility where video is recorded; this is accomplished through wired or wireless transmission, each with its own cost and technology limitations.

B. Wide Dynamic Range Cameras. These cameras are used in outdoor placements where the field of view includes areas that have a range of lighting conditions from bright light to dark areas. An example of this could be an alcove where shadows are present in the same field of view as a playground in the bright sunlight. In this case, you would want to be able to discern someone standing in the alcove as well as the children in the bright area of the playground. Wide dynamic range cameras can process both areas in the field of view differently providing images that meet the operational requirement and use case.

TIER 3

A. Infrared (IR) Cameras or Lighting. Supplemental lighting, via IR or visible light, refers to adding additional light to a scene to improve video surveillance image quality and usability after hours. Supplemental light can be either IR or visible light. IR lighting is invisible to the human eye but can be captured by a camera providing covert illumination of an area. The main drawback to this approach is that the images recorded and viewed are in black and white only and no colors are represented, which can impair situational awareness for surveillance, assessment and forensic use cases. Visible lighting illuminates an area with white light providing improved situational awareness with color images. There are many types of visible light luminaries, such as LED, halogen and fluorescent, but LED tends to offer long-term cost savings and better color rendition. Adding visible light to an area has the additional benefit of improving "natural surveillance" by human observers, which is a principle of CPTED.

Image sensor technology has progressed to the point where color imagery is possible in the near absence of visible light. For this reason, some school districts have reduced the use of supplemental lighting to decrease operating costs while still maintaining the operational requirement for the use case defined. This approach decreases natural surveillance, so schools need to evaluate if it is the right approach for them.

B. Wireless Video Data Transmission. Wireless data transmission is used when camera placement precludes the use of wired transport due to high costs or distance limitations of the network. There are many wireless technologies available for schools to consider with different network speeds or data transmission rates as well a distance or coverage area. A wireless audit of the school and surrounding areas should be conducted to ensure that wireless technology chosen does not interfere with other systems and vice versa. PASS recommends that a school should define the video surveillance use case and operational requirement before choosing a wireless technology to deploy. In this manner, a system can be designed around specific video surveillance needs that govern the bandwidth and distance requirements.

C. **PTZ Camera Coverage**. PTZ cameras provide a means for proactively assessing a specific area of interest by remotely moving the camera's field of view and focal length; they require personnel manually operating the camera in response to an incident alert. For this reason, PTZ cameras are a great tool for the assessment and surveillance use cases. They are of limited use if you do not have an operator but can be set to act as a fixed camera for a specific field of view when not being controlled. In some cases, PTZ cameras are set on a "guard tour" moving from one preset position to the next and providing video coverage of that area for a set amount of time. This way, one camera can cover multiple areas, but there is always the risk of a missed incident if the camera is covering a different area than that of the incident.

PTZ cameras should be rated for outdoor use to prevent ingress of dust or water and environmentally rated to function in both upper and lower temperature ranges. They should also include wide dynamic range sensors to ensure image usability.

D. **Loitering Detection Analytics.** This technology for risk mitigation use proactively notifies school security personnel when triggered. Loitering is a problem for schools, whether it is from students skipping class or trespassers on school grounds. In either case, video surveillance analytics can help mitigate the risk of loitering before it escalates into a more serious problem by alerting school security personnel that someone may be loitering in a specific area so that a response can be initiated if required. Implementation of this technology should follow the manufacturer's guidelines for camera selection and placement.

TIER 4

A. **Perimeter Video Analytics.** This technology uses cameras or sensors to detect a person or object crossing a demarcation point, such as a fence or property line, and proactively alerts school security personnel so that a response can be initiated if required. Implementation of this technology should follow the manufacturer's guidelines for camera selection and placement.
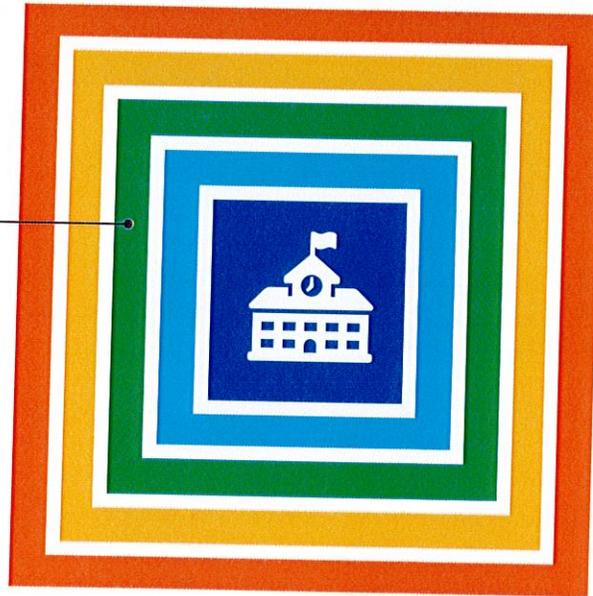
B. **People Identification at Gates or Points of Entry.** Video surveillance systems can be used at specific "choke points" for identification of people entering an area on school grounds, such as entry points to athletic fields, playgrounds or other areas where students, staff and visitors congregate for activities. Such cameras should be specified to meet the operational requirement of Identification defined above, rated for outdoor use to prevent ingress of dust or water and environmentally rated to function in both upper and lower temperature ranges. They should also include wide dynamic range sensors to ensure image usability.

PARKING LOT PERIMETER LAYER

» QUICKFIND

PARKING LOT PERIMETER LAYER

	TIER 1	TIER 2	TIER 3	TIER 4
• POLICIES AND PROCEDURES				
» Security Training for Staff and Volunteers	✔	✔	✔	✔
» Parking Tags	✔	✔	✔	✔
» Assign Staff to Periodically Check Parking Lot		✔	✔	✔
» Persistent Staff Patrol				✔
» RFID Parking Tags			✔	✔
» Staff Capability to Initiate Emergency Protocols From Exterior				✔
• ARCHITECTURAL				
» Apply CPTED Principles to Enhance Natural Surveillance	✔	✔	✔	✔
» Signage (Directing to Appropriate Areas)	✔	✔	✔	✔
» Signage Directing to Emergency Communication Device	✔	✔	✔	✔
• COMMUNICATION				
» Wide Area Mass Notification System (MNS)			✔	✔
» Two-Way Emergency Phones			✔	✔
» Audible and Visual Mass Notification Tied to District-Wide System				✔
• ACCESS CONTROL				
» Barrier Gates Integrated With Access Control				✔
• VIDEO SURVEILLANCE				
» Fixed Camera, Wide Area Coverage	✔	✔	✔	✔
» Wide Dynamic Range Cameras (when conditions require)	✔	✔	✔	✔
» People Identification Field of View at Pickup/Drop-off Area		✔	✔	✔
» Loitering Detection Analytics			✔	✔
» PTZ Camera Coverage			✔	✔
» Audio Analytics Integration				✔
» License Plate Recognition (LPR) and Data Integration				✔

PASS
Partner Alliance
for Safer Schools

POLICIES AND PROCEDURES COMPONENT:

TIER 1

A. **Security Training for Staff and Volunteers.** It is critical for a school district to empower staff and the community with security awareness in and around campus to include the parking lot perimeter. Early detection of a security threat generally relies on such measures as behavior-based surveillance (e.g., whether a person is acting oddly, dressed oddly or out of place). This can be accomplished by students, staff, volunteers and parents and requires that the school community embraces the "see something, say something" mentality, through an official program or other means, and for people to be generally aware of their surroundings. This concept can be applied to exterior areas, especially where staff, students and parents often begin and end their school days. Staff, volunteers and parents should also receive training on the proper flow and control of traffic in parking lots during drop-off and pickup times to help reduce the risk of vehicle-pedestrian accidents. While there is little to no cost associated with these Tier 1 measures, they can be some of the most important steps a school district can take to improve safety and security.

B. **Parking Tags.** Parking decals, stickers or numbered hang tags should be provided to staff members and regular volunteers and prominently displayed on their vehicles; however, these items should not display any information that would identify the employee or their position for their protection. A numbering or lettering system would be the best deployment.

TIER 2

A. **Assign Staff to Periodically Check Parking Lot.** Staff such as administrators, teachers and custodians assigned to check the parking lot should be equipped with radio communications back to the office. They should also be empowered to initiate an emergency protocol for the school if they detect a threat outside of the building and should be equipped with crisis de-escalation training for dealing with the public.

TIER 3

A. **Persistent Staff Patrol.** A trained staff member should be on duty to patrol the exterior of a school to include the parking lot perimeter at all times during normal operating hours to ensure that safety rules and other practices are being followed and check for unauthorized vehicles in the lot. The greatest benefit to having a person dedicated to this task is that they can focus solely on possible exterior threats of the facility. An assigned staff member should be equipped with radio communications and fully trained as a security officer. They should also be provided with a tablet or other portable device that provides access to data such as parking pass registrations and student information as needed. The device should also provide access to camera feeds and security system information. The assigned staff member can also be provided with a communications device that allows them to initiate a school in lockdown from the outside if a threat is detected approaching the building.

B. **RFID Parking Tags.** Employees use RFID stickers on vehicles for parking lot entry and exit (applicable as part of an access control system).

TIER 4

A. **Staff Capability to Initiate Emergency Protocols From Exterior.** All employees are provided with the technology and related training to report an emergency and initiate lockdown or other emergency protocols from outside the building through standalone devices, smartphone apps, etc.

ARCHITECTURAL COMPONENT:

Parking lots should have visual access from the main office area for staff to be able to observe vehicles and their occupants as they approach the building. If direct visual access is not possible, video surveillance capabilities should be employed to supplement situational awareness. Signage is an important component in directing visitors and others to proper areas on the school property.

TIER 1

A. **Apply CPTED Principles to Enhance Natural Surveillance.** Establish clear sight lines from perimeter windows to the parking lot by removing or trimming vegetation. For new construction, landscaping should be planned with clear sight lines in mind.

B. **Signage (Directing to Appropriate Areas).** Basic way-finding from the perimeter parking lot should be clear from any point within it. Signage is the most direct means of guiding building users and visitors to the appropriate point of entry. Signage is enhanced by indirect cues provided by thoughtfully designed landscape walkways, crosswalks and architectural elements at the desired building entry points.

C. **Signage Directing to Emergency Communication Device.** Signs should be posted that provide clear direction to an emergency communications device (if property is equipped), designed with an emergency and a user's likely state of heightened stress in mind.

COMMUNICATION COMPONENT:

Communication within the parking lot (or garage) area is similar to communication needs within the property perimeter layer. This layer is not normally attended by students, staff or visitors except for very short periods of time. This layer, however, still needs a communication mechanism to ensure that all persons with this layer are notified of a threat.

TIER 3

A. **Wide-Area Mass Nofication System (MNS).** The parking lot layer is considered within the area of a wide-area MNS. A wide area MNS is similar to weather emergency sirens with which many are familiar. The intent of the wide-area MNS is to provide a distinct signal to large areas within the school property to quickly inform the persons within the parking areas that a threat is imminent.

Recent advancements in wide-area sound technology provides districts the ability to use large speakers to easily provide a clear and intelligible message to parking areas. This technology can also be integrated with an emergency paging, fire alarm voice communication and/or intercom system.

B. **Two-Way Emergency Phones.** Depending on the size of the school campus, a parking lot area can encompass a vast amount of space that is difficult to monitor, providing a setting susceptible to threats. It is important to have some sort of two-way communication allowing the persons in the parking lot space to quickly communicate with the security team of the district.

Two-way emergency phones provide locations from which a person can communicate with the security team of the district. These emergency phones are normally placed strategically and in sufficient numbers so that one is accessible within 200 feet of any location within a parking lot.

These devices also have the capability to integrate with the video surveillance system to allow for audio and visual communication with security personnel. Use of this technology is particularly important within large campuses that have multiple parking areas.

TIER 4

A. **Audible and Visual Mass Notification Tied to District-Wide System.** As discussed earlier, most two-way emergency phones can be unified with other security systems. Such devices can be easily configured to send out emergency messages from the MNS and use a visual indicator atop the device for a visual representation of a threat. Districts are encouraged to investigate and implement this technology in a way that ensures baseline two-way communications but also allows a wide area MNS to provide clear and intelligible messages to the persons within the parking lot layer.

ACCESS CONTROL:

TIER 4

A. **Barrier Gates Integrated With Access Control.** Barrier gate systems can be very effective when integrated with an access control system. Barrier gates should operate very quickly, especially for parking lots and areas that have a lot of flow. Barriers should be made of material that will not damage a vehicle or cause injury from impact; however, schools may have to use slide-and-swing gates, which by nature are reinforced and impact resistant and in turn could cause damage to an inexperienced driver's vehicle and injury to the driver themselves.

Barrier gates can be integrated to work with a district's access control system. The preferred method can be using a proximity card to open the gate. This can be the same access card that is used by the district to open other access doors on schools. Cards can be programmed to only work with the gate card readers, so they could be issued to students. Sole keypad entry is a possibility but is less secure, as codes can be easily shared.

Automatic vehicle identification systems can also be used. This type of device requires little or no interaction by the driver, since a reader of the system will read the radio frequency signal as a vehicle approaches. In many cases, this is the safest type of system for pedestrians because the driver is not distracted.

Regardless of the solution, PASS recommends that any gate and access control system have a battery backup that allows the gate and access control system to continue to work in the event of a power or internet outage.

VIDEO SURVEILLANCE COMPONENT:

Whenever people and vehicles are combined in a confined area, the rate of accidents increases. As a result, parking lots are some of the most dangerous areas on school grounds. Video surveillance of this area should incorporate wide area coverage to record general activity and include cameras that can record resolutions that meet the identification guideline for specific pickup and drop-off areas.

Video surveillance is one component that can be used to mitigate risks for school parking lots by providing **surveillance, assessment, forensics and risk mitigation** as defined the district layer of the Guidelines.

Today, there are many different capability levels available in video surveillance equipment. Establishing an "operational requirement" for each camera deployed ensures the selection of equipment appropriate to the specific uses for which it is intended. These operational requirements are defined as:

- **Detection**—The ability to determine whether a person or object is in the field of view of the camera

- **Recognition**—The ability to differentiate and classify people and objects in the field of view of the camera (e.g., man or woman, child or adult, red or blue jacket, two cars and one truck)

- **Identification**—The ability to identify specific individuals or objects where present in the field of view of the camera (e.g., John Smith, a 2009 Toyota Camry, a license plate number)

Each of these operational requirements are defined by the number of "pixels on target" recorded of the object or person in the field of view. For a person, the number of pixels measured across the width of their face determines what operational requirement is achieved. While there are no established standards to define pixels on target to meet specific operational requirements, this chart outlines generally accepted thresholds in the security industry.

Operational Requirement	Horizontal Pixels/Face	Pixels per Inch
Identification	80	13
Recognition	20	4
Detection	4	1

Unless otherwise determined in a risk assessment, **recognition** and/or **detection** are the operational requirements for video surveillance of large outdoor areas.

TIER 1

A. **Fixed Cameras, Wide Area Coverage.** Fixed cameras provide video surveillance of outdoor activities taking place in the camera's field of view. Cameras should be rated for outdoor use to prevent ingress of dust or water and environmentally rated to function in both upper and lower temperature ranges.

The field of view should overlap the desired coverage area by at least one meter (when applicable) to ensure that the surveillance, assessment and forensics use cases are met. In some cases, cameras can be mounted directly on the building that houses the system's recording devices; this is the most cost-effective approach but can limit the field of view. Other mounting options include adding cameras to new or existing lighting poles around the property perimeter or on other buildings on the school property, such as athletic or maintenance structures. All these mounting options present the challenge of transmitting the video data back to the facility where video is recorded; this is accomplished through wired or wireless transmission, each with its own cost and technology limitations.

B. **Wide Dynamic Range Cameras**. These cameras are used in outdoor placements where the field of view includes areas that have a range of lighting conditions from bright light to dark areas. Wide dynamic range camera can process both areas in the field of view differently providing images that meet the operational requirement and use case.

TIER 2

B. **People Identification Field of View at Pickup/Drop-Off Area**. Video surveillance to cover the specific area where children are released to their parent or guardian, which will ensure that the school has a visual record of to whom a child was released. An ideal situation would be to pair this camera with a fixed camera, wide area coverage field of view to also record details of the vehicle used by the parent or guardian. In some cases, a higher-resolution camera with a wide area lens can provide both. These cameras should be specified to meet the operational requirement of Identification defined above, rated for outdoor use to prevent ingress of dust or water and environmentally rated to function in both upper and lower temperature ranges. They should also include wide dynamic range sensors to ensure image usability.

TIER 3

A. **Loitering Detection Analytics.** This technology for risk mitigation use proactively notifies school security personnel when triggered. A parking lot poses a unique challenge with loitering on school property since it is a common use area between known (students, staff, faculty and parents) and unknown individuals. Video surveillance analytics can help mitigate the risk of loitering before it escalates into a more serious problem by alerting school security personnel that someone may be loitering in a specific area so that a response can be initiated if required. Implementation of this technology should follow the manufacturer's guidelines for camera selection and placement.

B. **PTZ Camera Coverage**. PTZ cameras provide a means to proactively assess a specific area of interest by remotely moving the camera's field of view and focal length. This requires personnel manually operating the camera in response to an incident alert. For this reason, PTZ cameras are a great tool for the assessment and surveillance use cases. They are of limited use if you do not have an operator but can be set to act as a fixed camera for a specific field of view when not being controlled. In some cases, PTZ cameras are set on a "guard tour" moving from one preset position to the next and providing video coverage of that area for a set amount of time. This way, one camera can cover multiple areas, but there is always the risk of a missed incident if the camera is covering a different area than that of the incident.

PTZ cameras should be rated for outdoor use to prevent ingress of dust or water and environmentally rated to function in both upper and lower temperature ranges. They should also include wide dynamic range sensors to ensure image usability.
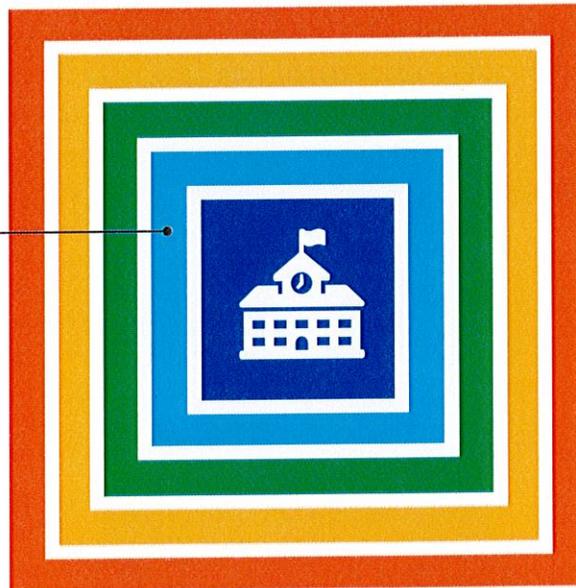
TIER 4

A. Audio Analytics Integration. Audio analytics involves the use of sensors and software that can detect and identify specific acoustic signatures of threat indicators, such as aggression or panic in people's voices and audible alarms. This technology can be loaded directly on the camera (as most network cameras already include a microphone), providing a dual-sensor technology capability within the same coverage area, or by using stand-alone devices that provide additional types of sensors. When triggered, an alert can be sent to designated safety and security staff to review the video and determine if a response is required. If incorporated on a camera, audio analytics are not limited by its field of view, so in some cases a trigger may require other means to verify a threat.

Many assaults are immediately preceded by a verbal argument, which can trigger audio analytics and possibly provide a timeframe for staff to respond before violence occurs. False alarms can be frequent with aggression and panic analytics since they can be triggered by children playing aggressively or shouting. Implementation of this technology should follow manufacturer's guidelines for sensor selection and placement.

B. License Plate Recognition (LPR) and Data Integration. LPR technology uses specific camera field of views to cover entry points for vehicles so that license plate data can be recorded. LPR solutions can provide the ability to enter license plate information for vehicles where notification to safety and security staff is needed upon entry, such as for vehicles belonging to individuals involved in custody issues for example. License plate data can also be processed through criminal and sexual offender databases to provide early warning to security and safety personnel as a related vehicle enters the property. Local laws and regulations may require sworn law enforcement personnel to be on staff to allow use of criminal and sexual offender databases. Implementation of this technology should follow manufacturer guidelines for camera selection and placement.

BUILDING PERIMETER LAYER

» QUICKFIND

PASS
Partner Alliance
for Safer Schools

BUILDING PERIMETER LAYER

	TIER 1	TIER 2	TIER 3	TIER 4
• POLICIES AND PROCEDURES				
» Categorization of All Exterior Openings	✓	✓	✓	✓
» Entrances Marked With First Responder Numbering System	✓	✓	✓	✓
» Policy Established for Control of Exterior Openings	✓	✓	✓	✓
» Key Control Procedures	✓	✓	✓	✓
» Complete Distributed Antenna System (DAS) Site Survey	✓	✓	✓	✓
• PEOPLE (ROLES AND TRAINING)				
» Staff Trained to Lock/Unlock Doors per Policy	✓	✓	✓	✓
» Visitor Management Policy/Process Training		✓	✓	✓
• ARCHITECTURAL				
» Signage (Directing to Appropriate Areas)	✓	✓	✓	✓
» Apply CPTED Principles Allowing Natural Access Control and Surveillance	✓	✓	✓	✓
» Secured Vestibule	✓	✓	✓	✓
» Emergency Building Access System for Fire/Law Enforcement	✓	✓	✓	✓
» DAS (New Construction/Renovation)	✓	✓	✓	✓
» One-Way Film on Exterior Windows to Prevent Visual Access	✓	✓	✓	✓
» Security Film on Exterior Door Vision Panels and Sidelites	✓	✓	✓	✓
» Ballistic Security Glass for Exterior Door Vision Panels and Sidelites			✓	✓
• COMMUNICATION				
» Public Address System	✓	✓	✓	✓
» Main Entry Door Intercom with Two-Way Communications		✓	✓	✓
» Audible and Visual Mass Notification Tied to District-Wide System				✓
» Unify Communication Systems With Video Surveillance and Access Control				✓
• ACCESS CONTROL				
» All Exterior Doors Secured With Lock or Exit Device	✓	✓	✓	✓
» Patented/Restricted Key System	✓	✓	✓	✓
» Key Management System	✓	✓	✓	✓
» Cylinder Dogging With Indicator	✓	✓	✓	✓
» Door Status Monitoring	✓	✓	✓	✓
» Electronic Access Control of Primary Entrances	✓	✓	✓	✓
• VIDEO SURVEILLANCE				
» Video Intercom at Visitor Entrance Points		✓	✓	✓
» Interior, Fixed Camera Coverage for All Entrance Points	✓	✓	✓	✓
» Wide Dynamic Range Cameras (When Conditions Require)	✓	✓	✓	✓
» Exterior, Fixed Camera Coverage at All Entry Points	✓	✓	✓	✓
» Loitering Detection Analytics at Entry Points		✓	✓	✓
• DETECTION AND ALARMS				
» Intrusion Detection System on all Exterior Access Points	✓	✓	✓	✓
» Intrusion Detection System Monitored 24/7	✓	✓	✓	✓
» Partitioned Intrusion Detection			✓	✓
» Automated Threat Detection				✓

PASS
Partner Alliance for Safer Schools

POLICIES AND PROCEDURES COMPONENT:

TIER 1

A. **Categorization of All Exterior Openings.** Every perimeter door should be classified as either primary, secondary or tertiary openings. Primary openings include main entrances and event entrances where the access to the building is both controlled and monitored. Secondary openings are primarily for emergency egress, although they may be required for access to the building in limited circumstances such as for employee entrances or access to and from playgrounds. These openings should be carefully controlled and never placed on any sort of automatic time schedule to open. Tertiary openings exist only for emergency egress and are not intended to be used for access to the building.

B. **Entrances Marked With First Responder Numbering System.** All entry doors should be clearly marked with the first responder door and window numbering system (see section on facility mapping under the district-wide architectural component), in coordination with local police and fire officials, to ease identification of entry points during emergency or tactical situations. Numbers should be made of reflective material like the numbers on a mailbox. In addition, the number system should be clear to the first responder as to where the door/window is within the relation of the school. For example, labeling a Door 1 of 21 or 121 allows first responders to decide which direction to go to find a specific door/window. Most first responders request the door/window labeling begin at the main entrance and proceed clockwise from the main entrance.[31]

C. **Policy Established for Control of Exterior Openings.** A policy should be set for governing when exterior doors are secured/unsecured. Per fire and building codes, all perimeter doors allow free exiting of the building in the event of a fire or other emergencies that require evacuation of the building. For entrance into the building, primary and secondary doors should have electronic access control or cylinder (if manual operation). Exit devices should have a visual indicator so that security and building personnel can look at the device and determine if it is in a secure condition. Additionally, these exit devices should allow for dogging (putting into an unlocked state) only by means of a key (policy should minimize the use of this practice, to the extent practicable).

Practical limitations related to existing buildings and the flow of students can make it very difficult to secure all perimeter doors. This is especially true at high schools with open campuses. All perimeter doors should be secured when students are in classrooms or when access from the exterior is not required for students to move from building to building. The number of doors unlocked during class changes should be limited. Any exterior doors that are unlocked during class changes should be monitored by a staff member or a SRO.

D. **Key Control Procedures.** Policies and procedures should be established to govern, track and revoke the distribution of keys and other access credentials as necessary. Keys should not be able to be duplicated without following a formal authorization process controlled by the district.

E. **Complete Distributed Antenna System (DAS) Site Survey.** A DAS is a technology to ensure that emergency first responder two-way communications systems will work inside the school, using a repeater or signal booster. Signal boosters may be required to ensure reliable radio communications both for campus staff and local emergency responders in stairwells, hallways, parking lots and other common areas where signals can be interrupted by building materials, dead spots and signal interference. A site survey to determine the need for this equipment can be conducted at no cost by local fire departments or radio manufacturers in many cases.

---

[31] Note—Law enforcement and fire approaches to identifying entrances are unified under *NFPA 3000—Standard for an ASHER Program* (2018)

PEOPLE (ROLES AND TRAINING) COMPONENT

TIER 1

A. **Staff Trained to Lock/Unlock Doors Per Policy.** Teachers, substitutes and other relevant staff should be trained on the proper procedures to lock and unlock primary and secondary doors at necessary times throughout the day. Electronic access measures (at higher TIER levels) can be used to supplement these procedures, facilitating class changes and other access needs.

B. **Visitor Management Process Training.** Admittance of all visitors, including vendors, parents, community members, substitute teachers and others who are not employed by the school, should follow a documented visitor management process led by main office personnel using a single point of entry. All relevant staff, including substitute teachers, should receive full training on the visitor management process.

ARCHITECTURAL COMPONENT:

TIER 1

A. **Signage (Directing Visitors to the Appropriate Areas).** Signage should be placed on every door indicating that all visitors must sign in at the front office and that individuals attempting to enter without authorization are subject to arrest.

B. **Apply CPTED Principles for Natural Access Control and Surveillance.** Exterior lights should be installed at strategic points on the building perimeter, illuminating the area during periods of darkness so that unauthorized and criminal activities are more easily recognized and deterred.

C. **Secured Vestibule.** The main (visitor) entry should be a secured vestibule with a mechanical lock or exit device as required by code and a doorbell. A staff member or authorized volunteer must assess a visitor's request to enter for any overt or suspected threat and then physically open the door or release it electronically if the opening is so equipped. The ability to visually assess the visitor is critical, whether directly or remotely (see intercoms in Communications and Video Surveillance).

D. **Emergency Building Access System for Fire/Law Enforcement.** A "Knox Box"-type system holds a master key or credential accessible only to fire departments, emergency medical services and law enforcement to allow rapid access to locked doors in emergency situations.

E. **Distributed Antenna System (New Construction/Renovation).** Two-way radio signal boosters may be required in new construction/renovation for compliance with the emergency responder radio coverage. DAS requirements are deemed necessary through a site survey. The evolution of new composite construction materials and wireless networks can interfere with the effective radio coverage for first responders. Schools can find more information on DAS through IFC-510 or NFPA-72, Chapter 24.

F. **One-Way Film on Exterior Windows to Prevent Visual Access.** One-way window film installed on lower classroom windows prevents visual access from the outside while allowing occupants clear visibility from the inside the classroom.

G. **Security Film for Exterior Door Vision Panels and Sidelites.** Security window film at least 14 millimeters thick (350 microns) should be installed on all exterior door vision panels[32] and sidelites.[33] Security film serves to deter or delay the ability of an attacker to breach a doorway using a firearm or other tool/weapon, in addition to limiting injuries from glass shards resulting from a blast, fire, accident, natural disaster or severe weather event. This type of solution can be retrofitted within most commercial window systems and incorporated into insulating glass units.

TIER 3

A. **Ballistic Security Glass for Exterior Door Vision Panels and Sidelites.** Several forms of security glass are available, incorporating acrylic, polycarbonate and other materials. Each has specific characteristics, weight and thickness depending on the intended use and level of ballistic resistance required. Security glass should be installed in all exterior door vision panels and sidelites that meets or exceeds the UL Level 3 standard for ballistic protection.

---

[32] Door vision panels are windows incorporated into a door.

[33] Sidelites are narrow windows immediately adjacent to a doorway.

COMMUNICATION COMPONENT:

TIER 1

A. **Public Address System**. As within the property perimeter layer, a school should have a one-way communication system reaching the areas immediately outside the building. In some cases, this will cover parking lots and playgrounds, but the priority for communication is for the areas in which student and staff would be outside near the building. These areas can include:

- Drop-off/pickup areas
- Sidewalks
- Bus loading and unloading areas
- Stand-alone mobile classrooms

B. **Main Entry Door Intercom With Two-Way Communications.** This is an example of an area where access control, video surveillance and communication can be unified into a comprehensive system (see Video Intercoms below). As discussed in the architectural element, the main entrance should be secured with a means to remotely unlock the door. The entry process consists of audible communication followed by use of access control and video surveillance systems, which provide staff the ability to remotely assess a visitor's request to enter and grant or deny access as dictated by policy or procedure.

TIER 4

A. **Audible and Visual Mass Notification Tied to District-Wide System.** The public address system that provides notification around the building perimeter should be a "zone" of the district-wide communication system to provide a way to deliver emergency communication from a district-wide perspective.

B. **Unify Communication Systems With Video Surveillance and Access Control.** Communication systems should be integrated with the access control and video surveillance to provide a unified security platform. The ability for school or district personnel to see what is happening around the building perimeter allows them to assess emergency situations and provide critical information the students and staff though communication systems. Additionally, unification with the access control system allows for doors to be locked and unlocked remotely.

ACCESS CONTROL COMPONENT:

Each school should invest in a plan to secure its building perimeter with an access control system that uses a combination of electronic and mechanical locks. Mechanical locks form the base for any access control system; however, electronic systems allow for historical and/or real-time tracking of ingress through secured doors, mitigates the expense of replacement of lost keys, allows for immediate deletion of access credentials when necessary and provides a means for the immediate lockdown of doors in the system.

Exterior doors should comply with appropriate locally enforced building codes for new educational occupancies, existing educational occupancies, new day care occupancies, existing day care occupancies, new business occupancies, existing business occupancies and ADA laws.

TIER 1

A. **All Exterior Doors Secured With Lock or Exit Device.** Every exterior door not routinely used for class changes (secondary/tertiary) should be secured with a working mechanical (or electronic) lock or exit device compliant with appropriate locally enforced building codes as well as the ADA. Tertiary openings should be exit only with no outside trim and should not have dogging mechanisms.

B. **Patented/Restricted Key System.** A patented or restricted key system offers protection against unauthorized key duplication by ensuring only authorized individuals can order key blanks and cut keys and cylinders for a key system. These common systems allow districts to control who has access to keys and can order them, which is a basic security function.

C. **Key Management System.** Requests for keys should be handled by a process in which each key distributed is logged and documented. Various types of systems and technologies are available to secure keys and track access and distribution.

D. **Cylinder Dogging With Indicator**. Where exit devices are provided with dogging feature (the ability to hold the exit device in an unlocked condition), the dogging mechanism should be the cylinder type with a visual indicator easily showing security staff whether the device is locked or unlocked.

E. **Door Status Monitoring**. All exterior doors should be electronically monitored for both door position and latch position; this allows staff to understand remotely if an opening is secure by knowing if a door is closed (door position) and latched (latch bolt position). It is especially important to monitor main entrance doors if the secured vestibule is not in direct view of the office or monitoring station.

F. **Electronic Access Control of Primary Entrances**. Exterior doors that are considered primary entrances should have electronic access control, both to limit the distribution of keys and to enhance the school's ability to control who can gain access to a specific building and when they can gain access. This access control also provides the ability for a school to audit who accessed a given opening and when. Required remote door release mechanisms should be by means of electric latch retraction for exit devices or electric locks. Use of electric strikes is not recommended.

VIDEO SURVEILLANCE COMPONENT:

Video surveillance is one component that can be used to mitigate risks at the building perimeter by providing surveillance, assessment, forensics and risk mitigation as defined the district layer video surveillance portion of the PASS guidelines. Having a visual record of people entering and leaving, and the activities they engage in at entrances, will provide another layer of deterrence for unwanted activities; it may also provide valuable situational awareness during emergencies.

There are many different capability levels available in video surveillance equipment. Establishing an "operational requirement" for each camera deployed ensures the selection of equipment appropriate to the specific uses for which it is intended. These operational requirements are defined as:

- **Detection**—The ability to determine whether a person or object is in the field of view of the camera

- **Recognition**—The ability to differentiate and classify people and objects in the field of view of the camera (e.g., man or woman, child or adult, red or blue jacket, two cars and one truck)

- **Identification**—The ability to identify specific individuals or objects where present in the field of view of the camera (e.g., John Smith, a 2009 Toyota Camry, a license plate number).

Each of these operational requirements are defined by the number of "pixels on target" recorded of the object or person in the field of view. For people, the number of pixels measured across the width of their face determines what operational requirement is achieved. While there are no established standards to define pixels on target to meet specific operational requirements, the following chart outlines generally accepted thresholds in the security industry.

Operational Requirement	Horizontal Pixels/Face	Pixels per Inch
Identification	80	13
Recognition	20	4
Detection	4	1

Unless otherwise stated or defined in a risk assessment, **identification** is the operational requirement for video surveillance of entrances at the building perimeter.

TIER 1

A. **Video Intercom at Visitor Entrance Points.** A video intercom should always be used when there is no direct line of sight to the person that is screening incoming visitors. These devices enable schools to speak with and observe visitors at the main entrance and any other areas, such as loading docks, where people other than students, faculty and staff need to enter the building. The use of networked video intercoms is recommended, enabling screening from multiple devices such as a monitor in the front office or on mobile devices if needed. Networked video intercoms can also be recorded on the VMS, providing a visual record of activities at entrance points. The intercom should be integrated with an electronic access control system to enable screeners to unlock the door remotely, regardless of the monitoring device they are using. Some districts require visitors to display a valid photo ID before the door is remotely unlocked, providing visual audit logs of people entering buildings, which can be compared with data in visitor management systems.

B. **Interior, Fixed Camera Coverage for All Entrance Points.** All video surveillance systems should provide a visual record of people entering the facility. Every exterior door should be included, even if it is always locked, since students or staff can easily open or prop doors from the inside to let someone enter the building, bypassing the requirement for screening at the main entrance.

There are generally two methods for configuring the field of view from these cameras:

1. Mount facing the door, thereby recording people entering the building

2. Mount facing the hallway, thereby recording people leaving the building and recording who they are taking with them, if applicable

It is preferable to mount cameras facing the door to record people entering the building to ensure schools have a visual record of someone entering (at a quality level allowing for identification), as the other cameras inside the building and outside the entrance, in many cases, can be used to determine if they were accompanied by someone else when leaving.

C. **Wide Dynamic Range Cameras.** Interior, fixed cameras at entrance points should be equipped with wide dynamic range sensors where the field of view includes areas that have a range of lighting conditions from bright light to dark areas. Glass entry doors are notorious for creating strong backlight conditions when the sun shines directly behind a subject walking through the door. Without wide dynamic range, a person's facial features are obscured in this situation, defeating the ability to identify who is entering the building. Wide dynamic range cameras can process both areas in the field of view differently, providing images that meet the operational requirement and use case.

TIER 2

A. **Exterior, Fixed Camera Coverage at All Entry Points.** Cameras should be mounted on the exterior wall of the school pointed towards all entry/exit points in a manner that provides the widest possible field of view of the area. In many cases, this will result in a profile view of the people existing the building. Where possible, due to the layout of the exterior walls, the cameras may have a direct forward-facing field of view which would be the preferred placement. This field of view provides a visual record of people loitering at exits and provides recordings of people entering the facility through entry points other than the main entrance. In most cases, this also provides a broad overview of school property just outside of the school perimeter, supporting additional uses. Exterior cameras should be rated for outdoor use to prevent ingress of dust or water and environmentally rated to function in both upper and lower temperature ranges. Outdoor cameras should also include wide dynamic range sensors to ensure image usability.

TIER 3

A. **Loitering Detection Analytics at Entry Points.** This technology for risk mitigation use proactively notifies school security personnel when triggered. Most schools do not have enough staff to effectively monitor all entrances to the facilities, creating opportunities for people to enter undetected if doors are opened from the inside. This scenario could be as innocent as a student letting another student in after opening bell, or it could be something worse; in either case, video surveillance analytics can help mitigate the risk of loitering before it escalates into a more serious problem by alerting school security personnel that someone may be loitering near entrances so that a response can be initiated if required. Implementation of this technology should follow the manufacturer's guidelines for camera selection and placement.

DETECTION AND ALARMS COMPONENT:

TIER 1

A. **Intrusion Detection System on All Exterior Access Points.** Each school building should be secured to protect against external threats when the building is unoccupied. PASS recommends an intrusion detection system that uses door position and latch bolt switches at each exterior door. In addition, exterior, large 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 that is used to arm and disarm the system. The intrusion system should also have 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.

B. **Intrusion Detection System Monitored 24/7.** As discussed in the district layer, every school building should have the intrusion system report to a central monitoring station; this allows for 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.

TIER 3

A. **Partitioned Intrusion Detection.** Intrusion systems also allow for the ability to secure interior portions of the building while some portions of the building are being used for other activities; this is called having "partitions" in the intrusion system. Through programming and design, the intrusion system can be set to have certain partitions armed while others are not.

For example, a school is having a basketball game in the gymnasium. While the gymnasium is being used by the public, the rest of the school should not be accessed. Intrusion system partitioning allows for the gymnasium to be used while sensors in other portions of the building will alarm to detect anyone who may enter unauthorized areas. This is an important aspect to intrusion for not just unauthorized entry, but also for other unique risks that schools face. Some examples are gang activity, bullying and illicit drug use. A properly installed intrusion system can help manage and deter threats to unoccupied buildings as well as when the building is occupied.

B. **Automated Threat Detection.** In advanced alarm implementations, various types of sensor technology and software can be used to detect and identify a range of threats at the building perimeter (such as gunshots), providing early warning of violence or potential violence (see also Audio Analytics). When triggered, an alert can be sent to designated safety and security staff to review and determine if a response is required. Implementation of this technology should follow manufacturer guidelines for sensor selection and placement.

CLASSROOM/INTERIOR PERIMETER LAYER
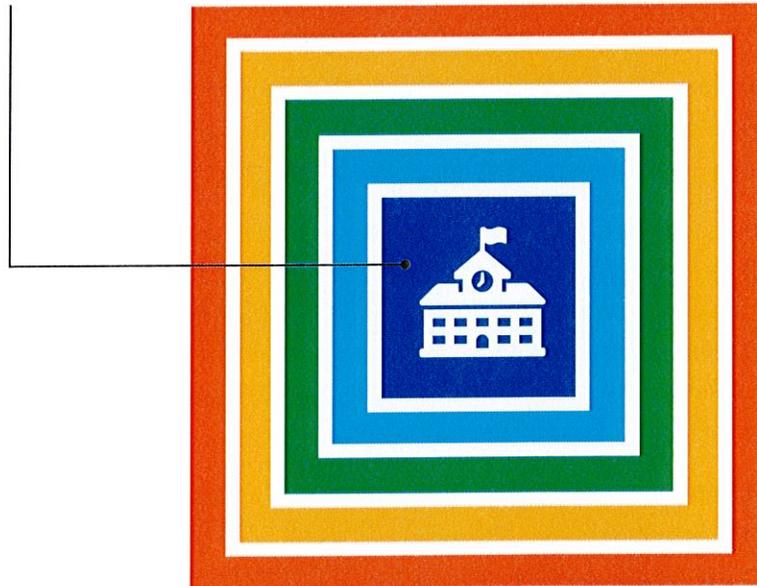
» QUICKFIND

CLASSROOM/INTERIOR PERIMETER LAYER

	TIER 1	TIER 2	TIER 3	TIER 4
• POLICIES AND PROCEDURES				
» Classroom Doors Closed and Locked When Occupied	✔	✔	✔	✔
• PEOPLE (ROLES AND TRAINING)				
» Teachers, Staff and Substitutes Trained on Emergency Protocols	✔	✔	✔	✔
• ARCHITECTURAL				
» Security Film on Door Vision Panels and Sidelites	✔	✔	✔	✔
» "Narrow-Lite" Style Classroom Doors with Blinds	✔	✔	✔	✔
» Compartmentalize Building with Cross-Corridor Doors	✔	✔	✔	✔
» Reinforced Walls at Shelter in Place Areas (New Construction)	✔	✔	✔	✔
» Safety/Security Optimization of Classroom Door Installation (New Construction)	✔	✔	✔	✔
• COMMUNICATION				
» Public Address System	✔	✔	✔	✔
» E-911 Added to Phone System (No Codes)	✔	✔	✔	✔
» Two-way Intercom System With Call Buttons		✔	✔	✔
» Duress Button System - Office and Classroom		✔	✔	✔
» In-Building Emergency Communication System			✔	✔
» Distributed Antenna System (DAS)			✔	✔
» Mass Notification Tied to District-Wide System			✔	✔
» Building-Wide Communication via Outside Calls (with record call option)				✔
» Use of Mobile Applications and Social Media				✔
• ACCESS CONTROL				
» Office, Storeroom or Security Classroom Function Locks	✔	✔	✔	✔
» Stand-Alone Electronic Locks With Fob			✔	✔
» Networked Electronic Locks				✔
• VIDEO SURVEILLANCE				
» Fixed Camera Coverage of All Common Areas	✔	✔	✔	✔
» Fixed Camera Coverage of Vestibule and/or Lobby Area	✔	✔	✔	✔
» Fixed Camera Coverage of Stairwells, Hallways and Restroom Entrances		✔	✔	✔
» Fixed Camera Coverage of Restricted Areas		✔	✔	✔
» Audio Analytic Integration			✔	✔
• DETECTION AND ALARMS				
» Intrusion Detection System Covering All Hallways and Public Areas		✔	✔	✔
» Intrusion and Duress (Panic) System Unified		✔	✔	✔
» Intrusion Detection System Covering All Classrooms			✔	✔
» Unified Communication and Detection System Monitored 24/7				✔
» Unified Communication and Detection System Monitored by District-Wide SOC				✔
» Alarms, Communications, Video Surveillance and Access Control Unified				✔
» Automated Threat Detection				✔

The most important assets to protect in a classroom (and on school grounds, for that matter) are students, staff, faculty and visitors. The security components within outer layers detailed in this guide also serve to protect classrooms and other interior areas of a school facility. These best practices relate to securing the classroom and shelter doors against active threats, unauthorized visitors and criminals. Shelter doors include areas of the building other than classrooms where building occupants could "shelter in place" during an emergency. These openings include gymnasiums, cafeterias, libraries, media centers, offices, teacher's lounges and auditoriums.

POLICIES AND PROCEDURES COMPONENT:

TIER 1

A. **Classroom Doors Closed and Locked When Occupied.** Classroom doors should be closed and locked when classes are in session or the rooms are otherwise occupied. Schools should work with first responders, local law enforcement and EMS to coordinate how access is gained to classrooms under the various TIER levels listed below.

PEOPLE (ROLES AND TRAINING) COMPONENT:

TIER 1

A. **Teachers, Staff and Substitutes Trained on Emergency Protocols.** Teachers and supervising staff have several important responsibilities before and during an emergency. Students will count on teachers and supervising staff to provide direction. The actions of teachers and supervising staff are integral to successful response in an emergency. Teachers must follow the directives of the site administrator/principal or their designee but also be able to act on their own in an emergency when direction is not available (see Policies and Procedures in the district-wide layer).

ARCHITECTURAL COMPONENT:

Architectural consideration and design are key components in the security and safety of building occupants. Classroom and other shelter in place locations, if designed correctly, can enhance safety through effectively deterring and delaying adversarial behaviors.

TIER 1

A. **Security Film on Door Vision Panels and Sidelites.** Security window film at least 14 millimeters thick (350 microns) should be installed on all classroom and shelter in place room door vision panels[34] and sidelites.[35] Security film serves to deter or delay the ability of an attacker to breach a doorway using a firearm or other tool/weapon, in addition to limiting injuries from glass shards resulting from a blast. This type of solution can be retrofitted within most commercial window systems and incorporated into insulating glass units.

B. **"Narrow-Lite" Style Classroom Doors With Blinds.** Classroom doors should include windows (narrow-lite style) for visual access both inside and outside the classroom. Blinds should be provided to cover these windows during a lockdown.

C. **Compartmentalize Building With Cross-Corridor Doors.** Interior cross-corridor doors should be used to confine an emergency event to a limited area of the building. These doors should normally be held open with electromagnetic devices that resist tampering and release upon activation of the lockdown process. Cross-corridor doors should be equipped with exit-only panic hardware and either a cylinder to manually gain access with a key or integration with an electronic access control system to electronically gain access.

D. **Reinforced Walls at Shelter in Place Areas (New Construction).** Reinforced walls in metal stud and drywall construction along shelter in place area of classroom.

E. **Safety/Security Optimization of Classroom Door Installation (New Construction).** Side walls near doors should be angled or beveled, as this will both 1) provide visual access that minimizes hiding nooks and 2) allow classroom doors to swing open toward the corridor for easy exit without impeding the movement of others in the corridor.

---

[34] Door vision panels are windows incorporated into a door.

[35] Sidelites are narrow windows immediately adjacent to a doorway.

PASS
Partner Alliance
for Safer Schools

COMMUNICATION COMPONENT:

TIER 1

A. Public Address System. At minimum, the building should have a public address system that can deliver emergency communications audibly and intelligibly to the interior of the building. Note: If a school has an older fire system that only has horns and not a voice-capable system, the horns can be used to create a different tone cadence to notify for a weather or active safety threat in the very similar manner as a fire alarm. It is recommended that public address systems be implemented in compliance with NFPA 72 Chapter 24 (see In-Building Emergency Communications System).

B. E-911 Added to Phone System (No Codes). Many enterprise phone systems require a code or number to be dialed before receiving a phone line to dial outside the facility. All phone systems should be set up so that no code or additional prefix number needs to be dialed for a 911 call.[36] This "E-911" feature ensures that anyone from any phone can dial 911 without any other actions.

C. Local Area Two-Way Radio System for Select Staff. A local area network radio system allows reliable voice communications between select staff on campus during an emergency in addition to day-to-day local school communications. At minimum, radios should be provided to key administrative staff, the front office and staff supervising the playground or other outdoor activities.[37] Commercial radio systems should be used rather than off-the-shelf consumer products or radios designed for recreational use. As noted in the district-wide layer, public schools as government entities must use radio systems licensed under the FCC Universal Licensing System.[38]

TIER 2

A. Two-Way Intercom System With Call Buttons. The public address system should be configured to provide a two-way intercom function allowing central locations to communicate with individual classrooms and individuals in the classrooms to communicate with the central locations.

B. Duress Button System—Office and Classroom. There are a variety of implementation options for duress alarm systems, sometimes referred to as panic alarms, which allow staff to immediately report specific threats that may begin in the classroom. This functionality should support the differentiation between various threats reported, allowing an all-hazard approach by including medical and other types of emergencies. The types of call buttons or other technologies used should be determined by needs identified through risk analysis.

C. Local Area Two-Way Radio System for All Staff, Including Teachers. A local area network radio system allows reliable voice communications between all staff on campus during an emergency in addition to day-to-day local school communications. As noted, commercial radio systems should be used rather than off-the-shelf consumer products or radios designed for recreational use.

---

[36] Relevant standards include National Electrical Manufacturers Association SB-40, Communications Systems for Life Safety in Schools.

[37] "The principal, vice principal, front office staff, playground supervisors, bus drivers, lunch duty staff, crossing guards and SROs should have these devices," DHS Primer to Design Safe School Projects, https://www.dhs.gov/xlibrary/assets/st/bips07_428_schools.pdf.

[38] For license example, see http://wireless2.fcc.gov/UlsApp/ApplicationSearch/applMain.jsp?applID=9075468.

TIER 3

A. In-Building Emergency Communication System. Requirements from the NFPA and the International Building Code (IBC) dramatically changed for K-12 schools in 2012. The IBC 2012 edition required that every new K-12 school have a one-way emergency communication system, per NFPA 72, Chapter 24, for not only fire threats, but also all hazards that affect a school.

Some of the key elements for a NFPA 72, Chapter 24-compliant system include:

- Intelligible audible communication in all areas in which staff and students occupy a space. "Intelligible" is defined as a clear, concise verbal signal that is easily understood. For practical purposes this means having public address speakers[39] in all classrooms, in addition to key shelter in place areas:

  — Hallways
  — Common areas
  — Library/media center
  — Auditorium
  — Gymnasium
  — Cafeteria

- There must be two locations from which a message can be communicated throughout a school building using the system—generally the main/front office and a secondary secure location.

- The communication system should have an alternate power source, whether this is battery backup, an uninterruptible power supply or a backup generator, in case of main power failure.

B. DAS. Signal boosters may be required to ensure reliable campus two-way radio communications and first responder radio coverage in stairwells, hallways and other common areas where signals can be interrupted by building materials, dead spots and signal interference (see DAS in the building perimeter layer). DAS systems can incorporate boosters for two-way radios and cellular phones. These are often referred to as in-building wireless solutions, which are typically custom designed for each unique environment.

C. Mass Notification Tied to District-Wide System. As described in within other layers, the in-building communication system should be integrated with the district-wide mass notification system. Within this integration, the school can receive instant alerts for weather and other emergencies that can affect the school.

There are a variety of technologies to interface the in-building communication systems to wide-area systems. Some of the way to unify the systems are as follows:

- **Hardwired Audio Connections:** This is a physical connection between the wide area notification system to the in-building communication system, like a hardwired microphone that is connected to the in-building system.

---

[39] Relevant standards include UL 2017, Standard for General-Purpose Signaling Devices and Systems.

- **Voice over IP (VoIP) Connection:** A VoIP connection allows audio transmission across a district's IT network. This connection can be made through a variety of technologies that include:

  - A VoIP phone system
  - Handheld radio to IP systems
  - Radio frequency to analog conversion systems

Since wide area communications systems are intended emergency communications with a large area such as a municipality, county or state; some states have adopted specific technologies or platforms to be used for such communications. For this reason, schools should work with local and state law enforcement to see what standards are in place before unifying communications technologies.

TIER 4

A. **Building-Wide Communication via Outside Calls (With Record Call Option).** During an emergency, it may become necessary for a first responder outside of the school to provide critical information to the staff and students inside the school. Two-way intercom systems can be configured to allow an outside call to trigger a mechanism to communicate a building-wide emergency message, allowing first responders to communicate to persons inside the building when they are incapable of reaching the main office or other area inside the school from which building-wide messages could otherwise be transmitted.

It is critically important for a system to record and log messages that are being announced during the emergency for review after the emergency event has ended. Every emergency event is an opportunity to learn how to better strengthen processes, procedures and technology to mitigate danger.

B. **Use of Mobile Applications and Social Media.** Emergency communications are most effective when they can be transmitted across multiple channels; however, it's important to ensure the most effective mechanisms received the highest implementation priority.

One well-known study[40] found that people best responded to communication in the following order:

- Phone call from a known person
- Live voice communication through a public address system
- Social media notification
- Text message notification

This data supports the conclusion of many life safety experts that the most efficient way to provide information in an emergency is through one-way live voice (and visual) communication systems; however, there are other communications mechanisms that can be very effective and offer certain advantages depending on the type of threat. Using multiple emergency communications methods supports an all-hazards approach to safety and security.

---

[40] "Organizational Communication in Emergencies: Using Multiple Channels and Sources to Combat Noise and Capture Attention," Stephens, Keri K. April 2013, eric. ed.gov/?id=EJ1004715

Mobile Applications: There are many applications that can be installed on mobile devices for staff and students to both alert the school or district to an emergency and receive emergency communications. Some applications can send video recordings and/or streaming in real time, while others can provide an alert that instantly notifies key personnel that a threat is in process. Some can even provide the location of the device via GPS. Administrators should ensure mobile applications are used in a strategic manner that conforms to the policies and procedures the school and/or district has in place.

Some considerations for evaluating mobile applications include:

- Does the application support communication emergency communication for all building occupants?
- What is the policy for mobile device use in the school? Mobile applications may be unable to provide timely to staff and students if mobile devices are not allowed to be used during class time.
- Is the cellular and/or wireless network capable of sending emergency notifications to hundreds or thousands of devices at one time?

Social Media: Nearly all schools and districts already have Twitter and/or Facebook accounts for the district, schools and school activities; however, each school should also have a social media account that is specific to emergency situations. This feed will allow the school and/or district to send information out to not only the students and staff, but also to parents and the surrounding community. A separate account for emergencies can assist in differentiating normal day-to-day postings from urgent information about emergency events.

ACCESS CONTROL COMPONENT:

While many types of mechanical and electronic locks are available, certain functionality is essential for classroom doors from a safety and security standpoint.

1. Any lock on a classroom door should have the ability to lock the outside lever from the inside of the room.[41]

2. Openings must allow keyed or electronic access from the corridor side for access by authorized personnel without a special tool or knowledge.

3. Free egress should always possible from the inside of the room. [42]

4. Locks should have a visual indicator so that the condition of the lock (locked or unlocked) is visible to room occupants.

Regardless of whether mechanical or electronic locks are installed at classroom and interior openings, interior doors should comply with appropriate locally enforced building codes for new educational occupancies, existing educational occupancies, new day care occupancies, existing day care occupancies, new business occupancies, existing business occupancies and the ADA. PASS recommends that school administrators work with local life safety experts to determine code compliance related to securing classroom doors.

TIER 1

A. **Office, Storeroom or Security Classroom Function Locks.** Classroom and other shelter in place room doors should be locked by means of either an office, storeroom or classroom function lockset or exit device as required by local codes.

- **Office function lockset:** The outside lever can be set in a locked or unlocked position by a push button lock feature on the inside lever, allowing the door to be easily secured from inside the room. Allows free egress from the inside of the room.

- **Storeroom function lockset:** The outside lever is always locked as a default position—so when the door is closed it is also locked. Allows free egress from the inside of the room.

- **Security classroom function lockset:** The outside lever can be set in a locked or unlocked position by a key in the inside lever, allowing a teacher to secure the door from inside the room. Allows free egress from the inside of the room.

The choice of which type of lock to use should consider the room's normal occupants and intended use, a facility assessment and any relevant state laws or local requirements.[43] As noted above, locks should always be keyed on the corridor side for access by authorized personnel. Here are some additional considerations:

---

[41] Recommended by the U.S. Department of Education and DHS; see DHS Primer to Design Safe School Projects, dhs.gov/xlibrary/assets/st/bips07_428_schools.pdf.

[42] Free egress generally means the door can be opened from the inside with a single motion and without the use of a key, special knowledge or effort.

[43] Some states require a specific type of lockset among these for classrooms; for more information, see idighardware.com/schools.

- Office function locks are simple to use, but this also allows anyone to lock the door from the inside of the room.
- Storeroom locks do not require an additional action to secure the door but will always require authorized personnel to open the door with a key from the outside of the room if needed.
- Many older classroom locks require teachers to step outside of the room to lock the door, which is unacceptable from a security standpoint. Security classroom function locks allow the teacher to lock the outside lever from the inside of the room with a key; however, this limits the locking of the door to authorized personnel who have keys.

TIER 3

B. **Stand-Alone Electronic Locks With Fob.** In electronic systems, doors should be equipped with a stand-alone electronic door lock that can be locked wirelessly from a fob or other device from anywhere in the classroom. Electronic stand-alone locks can be locked remotely with a fob or other electronic actuator, generally from up to 75 feet away; this should include a visual indicator allowing the condition of the lock (locked or unlocked) to be visible to room occupants. As noted before, locks should be keyed on with corridor side, with credential access by authorized personnel.

TIER 4

A. **Networked Electronic Locks.** In networked systems, doors are equipped with electronic locking systems that can be initiated both remotely from a central location or by a teacher in the classroom and tied into the school security system. Networked locks should also include a visual indicator allowing the condition of the lock (locked or unlocked) to be visible to room occupants. Some locks can also send a signal to a command center and/or lock down a pre-programmed section of the building if actuated locally.

VIDEO SURVEILLANCE COMPONENT:

Video surveillance can be used to mitigate risks for the classroom and interior perimeter by providing surveillance, assessment, forensics and risk mitigation as defined in the district-wide layer in the guidelines. Having a visual record of student, staff, faculty and visitor activity throughout the day provides another layer of deterrence for unwanted activities; it may also provide valuable situational awareness during emergencies.

There are many different capability levels available in video surveillance equipment. Establishing an "operational requirement" for each camera deployed ensures the selection of equipment appropriate to the specific uses for which it is intended. These operational requirements are defined as:

- **Detection**—The ability to determine whether a person or object is in the field of view of the camera

- **Recognition**—The ability to differentiate and classify people and objects in the field of view of the camera (e.g., man or woman, child or adult, red or blue jacket, two cars and one truck)

- **Identification**—The ability to identify specific individuals or objects where present in the field of view of the camera (e.g. John Smith, a 2009 Toyota Camry, a license plate number)

Each of these operational requirements is defined by the number of "pixels on target" recorded of the object or person in the field of view. For people, the number of pixels measured across the width of their face determines what operational requirement is achieved. While there are no established standards to define pixels on target to meet specific operational requirements, this chart outlines generally accepted thresholds in the security industry.

Operational Requirement	Horizontal Pixels/Face	Pixels per Inch
Identification	80	13
Recognition	20	4
Detection	4	1

Unless otherwise stated or defined in a risk assessment, **recognition** or **identification** includes the operational requirements for video surveillance within the classroom and interior perimeter, depending on specific use. Since these are indoor applications, at some distances identification can be achieved, but at longer distances, only detection will be possible.

TIER 1

A. **Fixed Camera Coverage of All Common Areas**. Video surveillance should cover all areas where students interact daily. These areas include cafeterias, libraries, gymnasiums, media, theaters and other common areas. Additional places to consider include areas where students and/or parents interact with staff, such as the main office or rooms that are used for parent-teacher conferences. Fixed domes are also preferable to traditional, box format cameras, which can be manually moved to point in a different direction than intended.

B. **Fixed Camera Coverage of Vestibule and/or Lobby Area**. Fixed camera coverage for the vestibule and/or lobby area should be implemented to provide a visual record of people entering the facility. The video intercom provides camera coverage of people approaching the entrance, while cameras mounted in the vestibule and lobby area record movement and activities as people enter the facility.

TIER 2

A. **Fixed Camera Coverage of Stairwells, Hallways and Restroom Entrances.** These areas are often identified in risk assessments as areas of concern, particularly in middle schools and high schools. Often, students loiter in stairwells between classes, making these areas important to cover. Incidents between students can occur in restrooms which, due to privacy considerations, cannot be covered by video surveillance, but it is appropriate to have a visual record of people entering and leaving these areas. Coverage of hallways is critical from a security and incident response perspective. Recognition is the operational requirement for video surveillance in these areas.

B. **Fixed Camera Coverage of Restricted Areas.** Access to certain areas within a school is restricted to authorized staff members, and the areas are usually secured behind a locked door. Video surveillance of these areas will provide a visual record of people entering and the activities taking place within them. Such areas can include server rooms, IT closets, maintenance closets and lab areas where chemicals are stored, for example. Identification and recognition are the operational requirements for video surveillance in these areas.

TIER 3

B. **Audio Analytics Integration.** Audio analytics involve the use of sensors and software that can detect and identify specific acoustic signatures of threat indicators, such as aggression or panic in people's voices and audible alarms. This technology can be loaded directly on the camera (as most network cameras already include a microphone), providing a dual-sensor technology capability within the same coverage area, or implemented by using stand-alone devices that provide additional types of sensors. When triggered, an alert can be sent to designated safety and security staff to review the video and determine if a response is required. If incorporated on a camera, audio analytics are not limited by its field of view, so in some cases a trigger may require other means to verify a threat.

Many assaults are immediately preceded by verbal arguments, which can trigger audio analytics and possibly provide timeframes for staff to respond before violence occurs. False alarms can be frequent with aggression and panic analytics, since they can be triggered by children playing aggressively or shouting. Implementation of this technology should follow manufacturer's guidelines for sensor selection and placement.

DETECTION AND ALARMS COMPONENT

TIER 2

A. Intrusion Detection System Covering All Hallways and Public Areas. While intrusion detection can be limited to the breach of the building from the outside, the addition of motion sensors inside the building assists as a second level of detection in case a breach happens that does not involve a door or window being breached. By covering hallways and public areas, the intrusion system can deter events such as theft and internal vandalism by persons who may "hide out" in the school building after the building closes.

The ability to monitor hallways and public areas also supports an all-hazard approach to safety in the event of an emergency. Responding to a weather threat, an intrusion system can be activated to alert administration to any movement in the areas where staff and students should not be during the weather emergency. The system also assists in active threat drills to see how quickly hallways and public areas are evacuated and in tracking a potential perpetrator while under an active threat scenario.

B. Intrusion and Duress (Panic) System Unified. An advantage of intrusion detection technology is the ability to add devices to the system in a cost-effective manner. One use of the intrusion system is to allow for duress buttons to be installed that can assist in implementing procedures for a variety of life safety threats. Buttons can be installed in the main office and other public areas that would immediately communicate and differentiate between different types of emergencies or threats.

TIER 3

A. Intrusion Detection System Covering All Classrooms. The use of detection within a classroom is two-fold. First, detection inside the classroom allows for an alert to be sent to administration when persons are inside classrooms during hours in which they should not be admitted; second, duress buttons can be added to the classrooms to allow for immediate alert to a security threat. As with adding duress buttons in the main office and public areas, these alerts can be easily extended into the classrooms.

Intrusion systems also have wireless capabilities allowing teachers to carry devices on their persons that can alert administration, district and possibly first responders that emergency events are taking place. Coordination with law enforcement and other first responders is recommended if the decision is made to implement such a system.

TIER 4

B. Unified Communication and Detection System Monitored 24/7. At the building level, administrators should investigate how other life safety and detection systems can be unified to provide an efficient way to activate emergency procedures and notify students, staff and visitors that a threat is imminent. For example, the intercom, fire alarm and paging systems can all be integrated with the intrusion system to provide instant alert of a threat. This unification allows monitoring by a central monitoring system. As with a fire alarm, a process should be in place to drill and train for the event protocol of monitoring the intrusion system 24/7.

C. **Unified Communication and Detection System Monitored by District-Wide SOC.** For districts that do have a SOC, it is important the intrusion system is monitored by the SOC, allowing the district to provide alerts and notifications district-wide or to individual schools. This allows the intrusion system to not just be used to provide information at the facility that has the event and also allows for processes to be implemented at other facilities, based on the threat detected.

D. **Alarms, Communications, Video Surveillance and Access Control Unified**. As districts implement intrusion detection technology, the goal should always be greater unification with other systems to provide the best protection for staff and students. For example, devices such as door position switches on the intrusion system can also be used with the access control system, as well as provide an input to the video surveillance system to tag activity at a door.

E. **Automated Threat Detection.** In advanced alarm implementations, various types of sensor technology and software can be used to detect and identify a range of threats indoors (such as gunshots), providing early warning of violence or potential violence (see also Audio Analytics). When triggered, an alert can be sent to designated safety and security staff to review and determine if a response is required. Implementation of this technology should follow manufacturer's guidelines for sensor selection and placement.

KEY RESOURCES

Partner Alliance for Safer Schools (PASS)
passk12.org

Door Security and Safety Foundation
lockdontblock.org

National Association of School Resource Officers—Resources and Best Practices
nasro.org/membership/resources

National Association of State Fire Marshals - Classroom Door Security and Locking Hardware
firemarshals.org/NASFM-Documents

National Center for Spectator Sports Safety and Security
ncs4.com

National Council on School Facilities
facilitiescouncil.org/ncsf-home

National Fire Protection Association (NFPA)
nfpa.org/Codes-and-Standards/All-Codes-and-Standards/List-of-Codes-and-Standards
NFPA 101—Life Safety Code
NFPA 72—National Fire Alarm and Signaling Code
NFPA 730—Guide for Premises Security
NFPA 731—Standard for the Installation of Electronic Premises Security Systems
NFPA 3000—Standard for an Active Shooter/Hostile Event Response (ASHER) Program

National Systems Contractors Association
nsca.org

Readiness and Emergency Management for Schools Technical Assistance Center
rems.ed.gov

Safe and Sound Schools: a Sandy Hook Initiative - Straight A Safety Improvement Toolkits
safeandsoundschools.org/programs-2/toolkits

Secure Schools Alliance—Research and Education
secureschoolresources.org

Security Industry Association
securityindustry.org

The Police Foundation—Averted School Violence Database
asvnearmiss.org

U.S. Department of Homeland Security—Building and Infrastructure Protection Series: Primer to Design Safe School Projects in Case of Terrorist Attacks and School Shootings (FEMA-428/BIPS-07)
dhs.gov/xlibrary/assets/st/bips07_428_schools.pdf

U.S. Department of Homeland Security—CCTV Technology Handbook
dhs.gov/sites/default/files/publications/CCTV-Tech-HBK_0713-508.pdf

PASS™

Partner Alliance
for Safer Schools

passk12.org

ABSOLUTE DEFENSE, LLC.
207-A EAST LEWIS STREET
GREENSBORO, NC 27406

ATTENTION: ANNIE B. TRENT
336-317-6286 (C) 336-274-1811 (O)