

School Security– A Best Practices Guide



**Massachusetts Chiefs of
Police Association
October 2023**

Introduction

Understanding that physical security and the hazards of the learning environment may be outside the skill set of professional educators, the law enforcement community in Massachusetts recognizes the need to provide 'best practices' for school administrators.

We understand that administrators are often inundated with conflicting and contradictory security recommendations, and that much of this information comes from non-reliable sources, or the security industry itself.

Our goal, is to present the academic audience, with real advice and recommended practices, that have proven effective. As our understanding of school security evolves, we may change or update this document as needed.

The Massachusetts Chiefs of Police Association is dedicated to life safety and the security needs of our school systems. We believe that working together, we can make our schools safer.

Executive Summary

The Massachusetts Chiefs of Police Association (MCOPA) has, as part of its committee structure, a group to address school security concerns. The members of that committee recognize the minefield of information that confronts school districts state-wide. Our initial intent was to draft a set of agreed upon recommendations that would serve as a map for all school districts in the state.

With this goal in mind, the MCOPA School Safety and Security sub-committee undertook a literature review of existing authoritative documents on the subject, to identify trends and universally accepted practices. A reference section to this report is included, but in general, the U.S. Department of Homeland Security, the Secret Service, and the Federal Commission on School Safety, offer the most guidance on this topic. There is clear consensus on the following:

1. Collaboration
School officials and law enforcement must have a working relationship before an event occurs. A team approach to school security offers an opportunity for law enforcement and school officials to collaborate and understand expectations before an incident happens.
2. Assessment
Each school district should have a multi-layered plan for all public schools. That plan starts with a risk assessment survey.
3. Prevention
The use of a 'threat assessment team' is a universal recommendation. Both law enforcement and school districts have strict privacy regulations, but school safety is paramount. School employees and law enforcement should work together to identify and avert threats. In essence, a threat assessment team is a group with

varying expertise that analyzes communications and behaviors to decide on whether or not an individual poses a threat to him/herself or others.

An anti-bullying campaign is also identified as a universal recommendation. Many incidents of violence have a bullying component.

Social media has a strong influence on student behavior. We recommend social media awareness and investigative capabilities for popular social media sites, which can identify concerning statements or potential violence before they happen.

4. Mitigation

This includes classroom hardening techniques, and education for students and staff. Schools should have well established evacuation plans with rallying points, as well as communication capability that can be used in emergencies.

Part of the communication plan may include a mass notification system. This includes the ability to communicate with students and parents, but also encompasses an on-site emergency network that utilizes geo-fencing and emergency buttons to notify key individuals of an emergency, and its location. The School Resource Officer, or 911 Center may be included in the notification group.

5. Response

Recommendations for response to a school-based emergency include getting key school staff members trained in Incident Command System (ICS). This is the system the law enforcement and Fire/EMS use to manage large incidents. Recommended by the federal government, ICS will provide emergency responders with a common framework to operate from.

At the minimum, school staff should understand the expectations that first responders have when responding to an incident, and be prepared to act as a resource and liaison to the unified command. Basic ICS training is a classroom introductory only.

The school systems should have a comprehensive emergency management plan that interconnects with the municipal/city plan. The Massachusetts Emergency Management Agency (MEMA) offers free assistance for this effort.

Recommendation

MCOPA seeks to produce a document that identifies evidence-based tactics and procedures, to be distributed to school districts throughout the Commonwealth. As part of this effort, we researched dozens of reports and publications, and identified recommendations with varying levels of expertise.

Many government agencies have produced reports that are available on-line (see below or 'References'). Unfortunately, most are theoretical in nature, offering little real-world advice. Homeland Security's "**K-12 School Security**", available at <https://www.dhs.gov/publication/k-12-school-security-guide> emphasizes the need to consider social issues, mental health, and bullying. The guide documents the threat assessment process.

The U.S. Secret Service "Enhancing School Safety Guide", available at https://www.secretservice.gov/sites/default/files/reports/2020-10/USSS_NTAC_Enhancing_School_Safety_Guide.pdf stresses the need for a comprehensive targeted violence prevention plan. Including a multidisciplinary threat assessment team. This approach uses a variety of disciplines. The intent is to assess concerning students or situations and assess the risk posed to the school community.

Another U.S. Secret Service product is "Protecting America's Schools" available at https://www.secretservice.gov/sites/default/files/2020-04/Protecting_Americas_Schools.pdf. This document provides a study of 41 incidents of targeted school violence, and the recommendations that resulted.

The result of our assessment is to follow the guidelines offered by the "Partnership Alliance for Safer Schools (PASS)". This organization, of which the Mass Chiefs of Police is a member, offers the most comprehensive guideline on how to achieve a greater level of security in every school, large or small, public or private. Some of the recommendations may not apply to higher education, but many will.

The PASS organization (<https://passk12.org>) was founded in 2014, and has as its mission to bring together expertise from the education, public safety and industry communities to develop and support a coordinated approach to making effective use of proven security practices specific to K-12 environments, and informed decisions on security investments. Their vision is to support efforts by communities throughout the United States to provide and sustain an effective level of security appropriate to each district and K-12 facility, recognizing that making schools safer is both achievable and urgently needed.

"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 6th edition, released in March 2023, builds upon the existing guidelines primarily with additional best practices for architectural elements and the use of communications systems that enhance emergency response capabilities and includes a new section that examines promising emerging technologies that have

garnered significant interest and have been piloted in schools, including vape detection and passive weapons screening technology”.

The PASS Guidelines identify and classify best practices for securing K-12 facilities in response to urgent needs for information identified by the education community. The guidelines include:

1. Specific actions that can effectively raise the baseline of security
2. Vetted security practices specific to K-12 environments
3. Objective, reliable information on available safety and security technology
4. Assessment of current security measures against nationwide best practices
5. Multiple options for addressing security needs identified, based on available resources
6. How to distinguish needed and effective solutions from sales pitches on unnecessary products

The PASS program offers a comprehensive ‘School Security Checklist’ for schools to assess their security position. It is recommended that school systems start with an evaluation of the current condition before implementing comprehensive changes.

PASS is a 501(c)(3) nonprofit organization that allows private sector participation as well as partnerships with other nonprofits, but does not recommend security technologies based on corporate partnerships.

Our goal at MCOPA, is to provide our Massachusetts school system partners with real world, evidence based, up-to-date information, regardless of authorship. As a result, we concur that the PASS guidelines are the most comprehensive currently available.



**Massachusetts Chiefs of
Police Association
School Safety and Security
Committee**

John Horvath, Rockport – Chairman
Craig Bailey, Amesbury
Brian Gill, Ayer
John Paciorek, Jr., Deerfield
Stephen R. McDonald, Duxbury
Bruce R. McNamee, Edgartown
Paul Francis, Essex
Edward A. Dunne, Falmouth
Michael A. Grace, Foxborough
Matthew J. Stone, Holliston
Robert Garriepy, Huntington
Roy Vasque, Lawrence

Todd Fitzgerald, Manchester-by-the-Sea
Charles Gray, North Andover
Mark L. Smith, North Brookfield
William E. Lyver, Northborough
Brian M. Clark, Norton
David Scott, Pepperell
Charles J. Femino, Somerville
Michael J. Bradley, Jr., Upton
Marc Montminy, Uxbridge
Jack Pilecki, Wellesley
Terence Delehanty, Winthrop

Special Thanks to:

Mark Leahy, Executive Director –
MCOPA

Dr. Thomas Scott - Massachusetts
Association of School Superintendents

Resources

[Active Shooter Preparedness](#), U.S. Department of Homeland Security (2017).

[Active Shooter Situations](#), U.S. Department of Education, U.S. Department of Homeland Security, U.S. Department of Health and Human Services, U.S. Department of Justice, Federal Emergency Management Agency, and Federal Bureau of Investigation (2013).

[Assigning Police Officers to Schools](#), Office of Community Oriented Policing Services, U.S. Department of Justice (2010).

[Beyond the Badge: Profile of a School Resource Officer - A Guide for Law Enforcement](#), Office of Community Oriented Policing Services, U.S. Department of Justice (2016).

[Beyond the Badge: Profile of a School Resource Officer - A Guide for School Communities](#), Office of Community Oriented Policing Services, U.S. Department of Justice (October 2016).

[Crime Prevention Through Environmental Design \(CPTED\) School Assessment \(CSA\)](#), Centers for Disease Control and Prevention (2017).

[Guide for Developing High-Quality School Emergency Operations Plans](#), U.S. Department of Education, U.S. Department of Homeland Security, U.S. Department of Health and Human Services, U.S. Department of Justice, Federal Emergency Management Agency, Federal Bureau of Investigation (2013).

[Implications for the Prevention of School Attacks in the United States](#), U.S. Secret Service and U.S. Department of Education (2004).

[Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks](#), Federal Bureau of Investigation (2016).

[Mitigation for Schools and School Districts Fact Sheet](#), Readiness and Emergency Management for Schools (REMS), U.S. Department of Education (2017).

[Options for Consideration Active Shooter Preparedness Video](#), U.S. Department of Homeland Security (2017).

[Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide](#), Interagency Security Committee (2015).

[Prevention for Schools and School Districts Fact Sheet](#), Readiness and Emergency Management for Schools (REMS), U.S. Department of Education (2017).

[Primer to Design Safe School Projects in Case of Terrorist Attacks and School Shootings](#),

U.S. Department of Homeland Security (2012).

[Protection for Schools and School Districts Fact Sheet](#), Readiness and Emergency Management for Schools (REMS), U.S. Department of Education (2017).

[Recovery for Schools and School Districts Fact Sheet](#), Readiness and Emergency Management for Schools (REMS), U.S. Department of Education (2017).

[Response for Schools and School Districts](#), Readiness and Emergency Management for Schools (REMS), U.S. Department of Education (2017).

[Safe School-Based Enforcement through Collaboration, Understanding, and Respect: Local Implementation Rubric](#), U.S. Department of Education and U.S. Department of Justice (2016).

[Safe School-Based Enforcement through Collaboration, Understanding, and Respect: State and Local Policy Rubric](#), U.S. Department of Education and U.S. Department of Justice (2016).

[States' Roles in Keeping Schools Safe: Opportunities and Challenges for State School Safety Centers and Other Actors](#), Mary P. Carlton, Phelan Wyrick, Nadine Frederique, and Basia Lopez, National Institute of Justice, U.S. Department of Justice (2017).

[Threat Assessment in Schools: A Guide to Managing Threatening Situations and to Creating Safe School Climates](#), U.S. Secret Service and U.S. Department of Education (2004).

[Violence Prevention in Schools: Enhancement through Law Enforcement Partnerships](#), Federal Bureau of Investigation (2017).

[Youth Preparedness Catalog](#), Federal Emergency Management Agency (2016).

School Safety Plan Evaluation Tool for K12 Schools." Safe Havens International. <https://safehavensinternational.org/wp-content/uploads/2014/08/>

K12_School_Crisis_Site_Planning_Evaluation_Tool.pdf
 "Conducting a Security Evaluation." National Association of Independent Schools. <https://www.nais.org/articles/pages/conducting-a-securityevaluation.aspx>

"School Safety and Security," Op. cit. [2] "School Safety and Security Checklist." Partner Alliance for Safer Schools, 2018. pp. 2-7.
<https://passk12.org/guidelines-resources/>

"A Comprehensive Report on School Safety Technology." Johns Hopkins Applied Physics Laboratory, Johns Hopkins School of Education, Johns Hopkins Bloomberg School of Public Health, and National Institute of Justice, U.S. Department of Justice, October 2016. p. 2.2.
<https://www.ncjrs.gov/pdffiles1/nij/grants/250274.pdf>

“Safety and Security Guidelines for K-12 Schools.” Partner Alliance for Safer Schools, 2018. p. 13.

<https://passk12.org/guidelines-resources/pass-school-securityguidelines/>

Hill, G. “Properly Trained School Security Guards.” Security Today, March 2, 2015.



PASS
Partner Alliance
for Safer Schools

Safety and Security
GUIDELINES
for K-12 Schools

CONTENTS

I. About PASS	3	d. Communication Component	45
II. Introduction	4	e. Video Surveillance Component	46
a. Scope	5	V. Parking Lot Perimeter Layer	49
b. Structure of the PASS Guidelines	6	a. Parking Lot Perimeter Layer Checklist	50
c. Baseline Practices and Obligations	8	b. Policies and Procedures Component	51
d. Recommended Uses	11	c. Architectural Component	52
e. Risk Assessment – A Prerequisite	13	d. Communication Component	52
f. Layers of Protection	15	f. Video Surveillance Component	53
g. Safety and Security Components	16	VI. Building Perimeter Layer	55
h. Using the PASS Guidelines to Formulate a Comprehensive Security Plan	18	a. Building Perimeter Layer Checklist	56
III. District-wide Layer	20	b. Policies and Procedures Component	57
a. District-Wide Layer Checklist	21	c. People (Roles and Training) Component	58
b. Policies and Procedures Component	22	d. Architectural Component	58
c. Visitor Management System	28	e. Communication Component	59
d. Student and Staff Identification	30	f. Access Control Component	60
e. Architectural Component	31	g. Video Surveillance Component	61
f. Communication Component	33	h. Detection and Alarms Component	63
g. Weather Monitoring	34	VII. Classroom/Interior Perimeter Layer	64
h. Access Control Component	35	a. Classroom/Interior Perimeter Layer Checklist	65
i. Transportation	35	b. Policies and Procedures Component	66
j. Video Surveillance Component	37	c. People (Roles and Training) Component	67
k. Detection and Alarms Component	39	d. Communication Component	68
IV. Property Perimeter Layer	41	e. Access Control Component	72
a. Property Perimeter Layer Checklist	42	f. Video Surveillance Component	74
b. Policies and Procedures Component	43	g. Detection and Alarms Component	75
c. Architectural Component	44	VIII. Key Resources	81

DISCLAIMER: The *Safety and Security Guidelines for K-12 Schools* (the “Guidelines”) are provided for informational purposes only. Under no circumstances do the contributors to this document and organizations participating in the Partner Alliance for Safer Schools (PASS) provide any related guarantees or accept liability for any loss or damage resulting from any person acting or refraining to act on this information. The Guidelines are not a substitute for legal, financial and other professional advice that may be required to address the specific facts and circumstances related to the implementation of a particular 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 sixth edition (2022) 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 44 active shooter incidents from 2000 to 2019¹ 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/file-repository/active-shooter-one-page-summaries-2000-2018.pdf/view>;
<https://www.fbi.gov/file-repository/active-shooter-incidents-in-the-us-2019-042820.pdf/view>

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 assessment² or policies related to firearms. Likewise, many areas of response and recovery are within 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 (NASRO) provide excellent resources on the issues and best practices that are specific to personnel.⁴

While the safety and security of school facilities plays a key role in promoting safe and positive school climates, this should be part of a comprehensive school safety strategy that addresses other factors as well. For example, an assessment of targeted school violence by the U.S. Secret Service⁵ found that while there is no profile for perpetrators, 80% of student attackers were bullied by their classmates, indicating the importance of processes and procedures to intervene when such behaviors are reported.

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 countermeasures such as tactical equipment or arming staff or security personnel, on which current practice and community viewpoints vary considerably among states and regions.

Common Acronyms in School Security

ACS – Access Control Systems

CPTED – Crime Prevention Through Environmental Design

DAS – Distributed Antenna System

EOP – Emergency Operations Plan

ICS – Incident Command Center

IDS – Intrusion Detection System

MNS – Mass Notification System

MOU- Memorandum of Understanding

NCS4 – National Center for Spectator Sports Safety and Security

NFPA A.S.H.E.R. – Active Shooter/Hostile Event Response

NRF- National Response Framework

NTAC – National Threat Assessment Center

PASS – Partner Alliance for Safer Schools

SOC – Security Operations Center

VMS – Visitor Management System

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/>

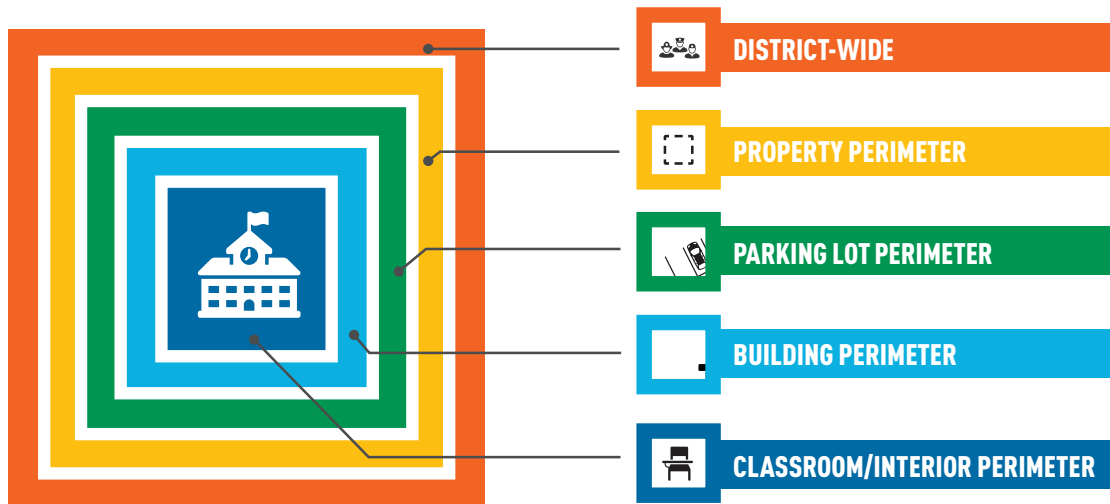
⁵ https://www.secretservice.gov/data/protection/ntac/Protecting_Americas_Schools.

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),⁶ the Guidelines describe approaches within five physical **layers** for school facilities.

LAYERS OF PROTECTION



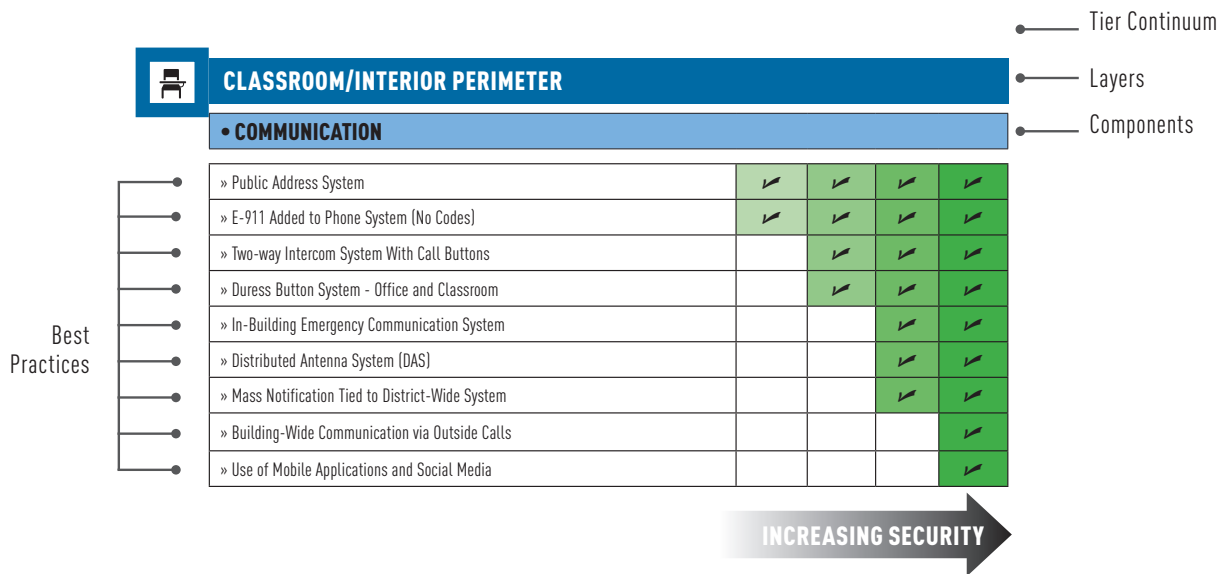
A layered approach is essential to addressing a broad range of threats, as each successive layer provides specific components to deter, detect or delay and respond to adversarial behaviors in the event that other layers are bypassed or breached. Each layer includes basic protective elements, or **components**, 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

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 within each layer.

⁶ DHS Primer to Design Safe Schools Projects (2012), dhs.gov/xlibrary/assets/st/bips07_428_schools.pdf



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.

TIER DEFINITIONS

Tier One: Establishes a foundation that is a baseline layer of security. All schools should work towards adherence to Tier One measures. Some Tier One standards have a minimal budgetary impact, while others require funding and the development of an implementation plan.

Tier Two: Builds upon the foundation laid in Tier One. Tier Two recommendations can be phased in with available funding and as local culture shifts towards heightened levels of security. All schools — regardless of size, location or other specific factors — should work toward adherence to Tier Two measures if Tier One is complete.

Tier 3: An implementation step for a higher level of security developed after a documented assessment by the core security team. The team should consider threats, local conditions, and available technology solutions with budgetary and staffing resource allocation.

Tier 4: An implementation recommendation that is part of an overall strategic security plan detailed by the core security team. Tier 4 recommendations often require multi-year planning and district-level funding for full implementation.

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.

Baseline Practices and Obligations

Some states have specific safety requirements applicable only to schools within their jurisdiction, such as Alyssa’s Law which has been adopted in at least three states so far (Florida, New Jersey, and New York) that requires the installation of panic alarms linked to law enforcement. Another example would be specific state laws regarding classroom locking mechanisms. At the same time, some safety measures—many procedural—are already required by federal law or regulation, or are commonly implemented throughout the U.S. Many (but not all) of the most relevant of these are highlighted here as “Baseline Practices and Obligations.” It is assumed in the Guidelines that all such legal and/or regulatory obligations and common practices are being met. The “best practice” recommendations across the Guidelines’ layers and tiers are understood to extend beyond what is legally required already and that school and district staff are aware of and implementing any additional state-specific requirements in conjunction with recommended best practices found in the Tier Continuum.

- **School and District Emergency Roles & Responsibilities Defined.** Each school district adopts the NRF and NIMS developed by the Federal Emergency Management Agency (FEMA), which establishes an Incident Command System (ICS), collaborative planning teams, and emergency operations plans (EOPs) that include any elements that are required by state law and should detail the role of safety and security technologies during an emergency.
- **All Staff Can Initiate Emergency Procedures.** All school staff should be able to initiate lockdowns and other emergency procedures when appropriate. During an active threat incident where there is a danger to occupants of a school, staff need to know how to reduce risk and protect lives until help arrives.
- **Empower Community to Share Concerns Through Anonymous Reporting.** Most districts use communications tools allowing students and others in the community to anonymously report potential threats and other concerns has demonstrated success in preventing potential violence. Some states, such as Colorado, mandate that public schools implement tip line programs.⁷
- **Staff and Volunteer Training 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.
- **Sharing Maps and Other Facility Information with Law Enforcement, Fire and EMS.** As schools present unique challenges for 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.
- **Security Plans Specific to Auxiliary Buildings.** Safety and security are just as necessary and important at school district auxiliary buildings (transportation centers, educational centers, warehouses and other places in a school district that are not considered instructional facilities) as they are at main instructional buildings.
- **Student Identification Badges (in secondary schools).** Identification badges are a simple and secure way to easily determine who is supposed to be on campus as long as 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.

⁷ Safe2Tell Colorado, safe2tell.org/?q=safe2tell-colorado-mobile-app.

- **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. For national context, see the nationwide survey conducted annually by Safe and Sound Schools.⁸
- **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 the use of automatic external defibrillators at a minimum. Many other first responder training programs are available that are relevant to trauma, mental health and other needs which arise during emergency situations.
- **All-Hazard, Scenario-Based Drills with Community Partners on Recurring Basis.** This type of exercise is intended to generate discussion of various issues regarding a hypothetical, simulated emergency and should foster an understanding of incident command and your district’s capabilities.
- **Video Data Use and Retention Policy.** A video surveillance use and data retention policy is typically established at the district level to ensure consistency across all schools. The use policy provides 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. 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.
- **Memorandums of Understanding (MOUs) with Emergency Responders.** Districts establish MOUs with local police, fire and EMS in two primary areas relating to emergency communication, threat information sharing and building access in an emergency.
- **MOUs With Law Enforcement for Sharing Video Data.** Districts also establish MOUs with local law enforcement to provide for sharing recorded or live video of incidents when necessary for emergencies and investigations.
- **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 are governed by MOUs so that roles and responsibilities are clearly defined and all parties can be adequately prepared to act if needed.
- **District Cybersecurity and Network Infrastructure.** The following measures are taken at the district level to address risks and help prevent both cybercrime against the school community and compromise of physical security systems via cyberattack.
 - **Cybersecurity best practices training for staff.**
 - **Routine data backups.** Core servers and data should be backed up and stored off-site for easier recovery in the event of an attack.
 - **Phishing filtering, testing, and simulation training.** “Phishing” is still the #1 delivery method for ransomware, having an effective campaign with employees is critical to protecting school networks.

⁸ <https://safeandsoundschools.org/2022/07/25/state-of-school-safety-report-reveals-students-want-more-social-and-emotional-support-and-increased-safety/>

- **Multifactor authentication or strong passwords.** Enable multi-factor authentication or other measures like strong password requirements, for access to teacher and education networks.
- **Device password change schedule for IP-based security equipment.**
- **Secure file sharing.** Secure files and records should not be sent by email.
- **Data loss prevention (DLP).** An effective data loss prevention program can alert the school if records are being accessed by an unauthorized source.
- **Network segmentation.** Networks are segmented to prevent the spread of malware on the network. Physical security networks should be separate from administrative and student networks.
- **Endpoint detection and response (EDR) solutions on devices.** Malware and endpoint detection and response is provided for all endpoints.
- **Mobile device management (MDM) or mobile application management (MAM).** Manage remote devices or applications through policies.
- **Implement all available software patches and vulnerability remediation.** This includes ensuring security equipment software and firmware is up to date.
- **Network monitoring using security information and event management (SIEM).** These systems enable security information and event management for early detection and response in the case of malware.
- **Vendor assessments.** Evaluating software vendors ensures they are providing adequate security and protection for schools.
- **Penetration testing, intrusion detection and compromise assessment.**

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 PASS 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 government⁹ 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. For more information on funding sources, see the Security Industry Association's Guide to School Security Funding.¹⁰

- **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.¹¹ 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.

⁹ The U.S. Department of Justice School Violence Prevention Program, cops.usdoj.gov/default.asp?Item=2958

¹⁰ <https://www.securityindustry.org/report/sia-guide-to-school-security-funding/>

¹¹ The U.S. Department of Justice School Violence Prevention Program, cops.usdoj.gov/default.asp?Item=2958.

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.¹²
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 lockset, such devices are typically offered as a lowest-cost lockdown solution. These devices can increase liability and risk and most violate fire and life safety codes as well as the Federal Law – Americans with Disabilities Act (ADA). For further information see *5 Reasons Schools Should Avoid Classroom Barricade Devices*¹³ and the *PASS Whitepaper on Classroom Barricade Devices*.¹⁴



Examples of “barricade” or “door blocker” devices.

¹² Rural Trust Special Report on School Violence, 2013, ruraledu.org/articles.php?id=3082

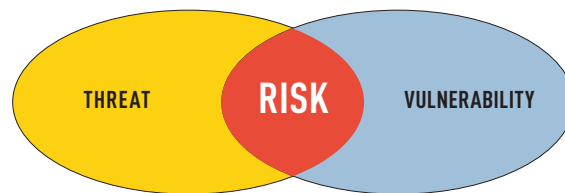
¹³ <https://passk12.org/news/5-reasons-schools-should-avoid-classroom-barricade-devices/>

¹⁴ <https://passk12.org/wp-content/uploads/2019/04/PASS-WHITEPAPER-Classroom-Barricades-2019-04-10.pdf>

Risk Assessment

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, protecting a facility and its occupants is viewed not as a reactive law enforcement function, but as a proactive security function. As mentioned earlier, the security objective is to deter, detect or delay, and respond to adversarial behavior through the use of people, processes and technology. The PASS components help mitigate risk by reducing vulnerability.

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 advisors¹⁵
- 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. It is an inventory of existing components that are identified in the PASS Guidelines and helps document any potential gaps in a school's protection efforts. 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 available¹⁶ 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.

¹⁵ For more information, see dhs.gov/protective-security-advisors.

¹⁶ Secureschoolresources.org/education-facilities-assessment

Similar free resources are also provided by state governments¹⁷ 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).

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 an 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.

¹⁷ 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.

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.

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 event 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,¹⁸ are two of many examples in which these routine communication technologies failed during emergency situations.

¹⁸ 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 prevent 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.

A NOTE ON TESTING

All technologies within the safety and security components (Communication, Access Control, Video Surveillance and Detection and Alarms) should be tested yearly. These tests can be carried out during the summer to ensure that all technology is functioning appropriately. Additionally, it is recommended that all IP-based technologies should be checked for failures each week. For example, a process should be in place to ensure that all video surveillance cameras are online and functioning properly.

Routine maintenance should be considered for all technology that has IP-based equipment, firmware, and software. Many systems require firmware and/or software updates. Districts/Schools should have a process to ensure that the current firmware and software versions are installed.

Using the PASS Guidelines to Formulate a Comprehensive Security Plan

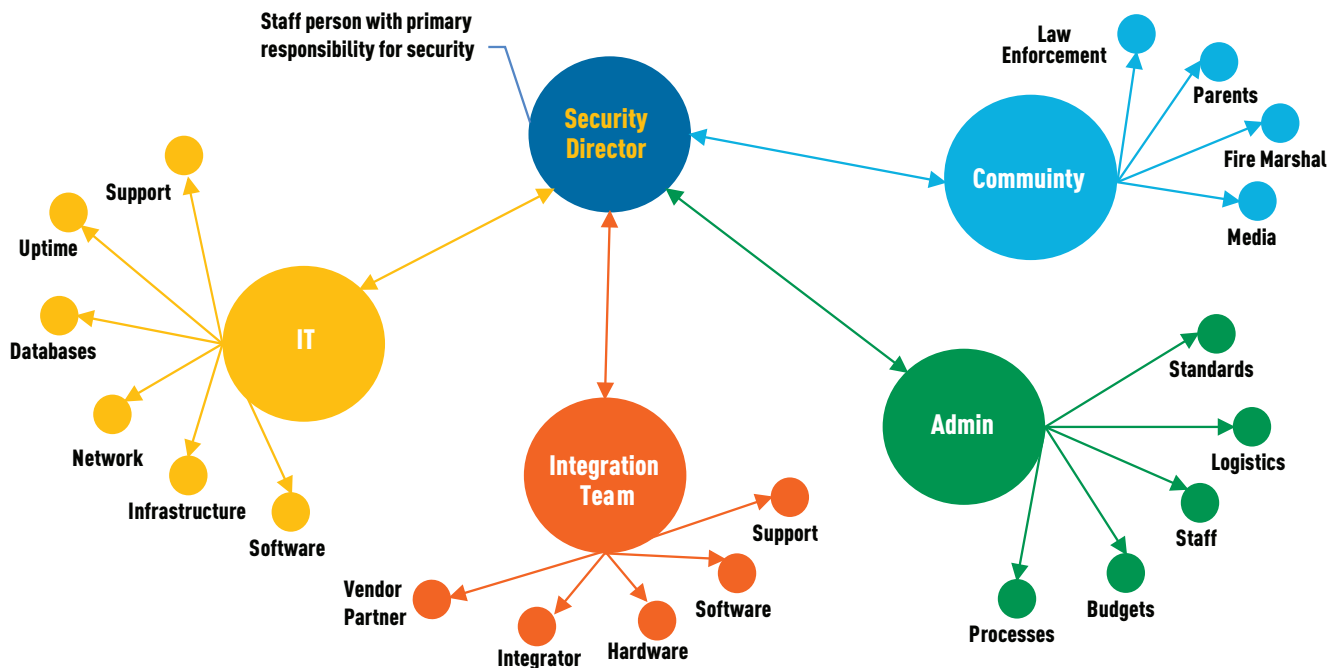
Here is a suggested roadmap for using the Guidelines to formulate a security management plan.

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
6. School-based health care professional

In larger or more complex projects, it is also best to have a hardware consultant involved in the process.


Security...It takes a team.



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:

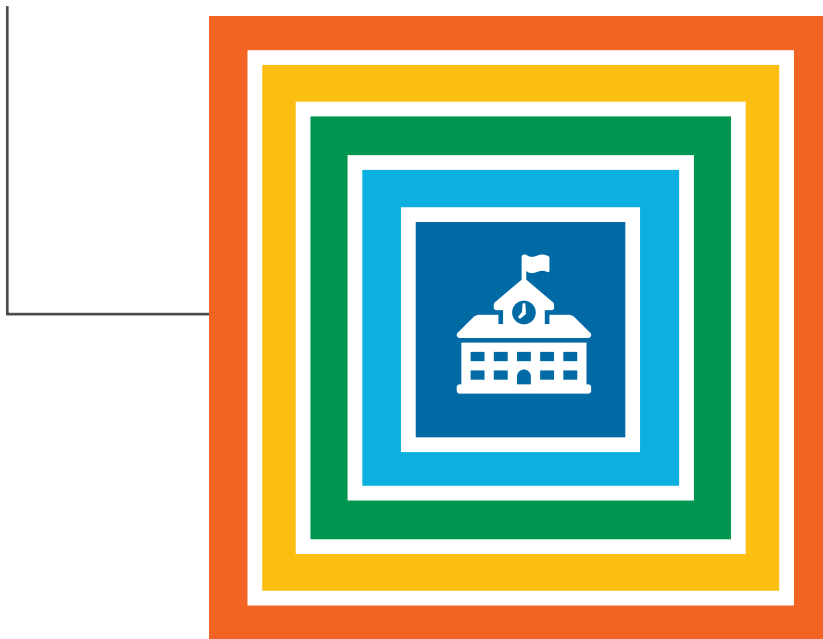
- Property Perimeter Layer
- Parking Lot Perimeter Layer
- Building Perimeter Layer
- Classroom/Interior Perimeter Layer

LAYER/COMPONENTS/BEST PRACTICES	TIER 1	TIER 2	TIER 3	TIER 4	Status	Year	Notes
 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 an estimated cost range for each best practice.



DISTRICT-WIDE LAYER



» QUICKFIND

District-Wide Best Practices	20	Weather Monitoring	34
Policies and Procedures Component	22	Access Control Component	35
Visitor Management System	28	Transportation	35
Student and Staff Identification	30	Video Surveillance Component	37
Architectural Component	31	Detection and Alarms Component	39
Communication Component	33		



DISTRICT-WIDE LAYER

• POLICIES AND PROCEDURES

	TIER 1	TIER 2	TIER 3	TIER 4
» Dedicated Security Director/Department	✓	✓	✓	✓
» Establishment of Safety Policies and Procedures	✓	✓	✓	✓
» District-Wide Physical Security Standards	✓	✓	✓	✓
» Annual Physical Security Assessments Based on District-Wide Standards	✓	✓	✓	✓
» Pre-Approval of Applications for School-Issued Electronic Devices	✓	✓	✓	✓
» Ensure Maintenance of Security Technology Implementations	✓	✓	✓	✓
» Conduct Lockdown Drills	✓	✓	✓	✓
» Independent Security Assessment on 3-Year Cycle				✓

VISITOR MANAGEMENT SYSTEM

» Visitor Badging System	✓	✓	✓	✓
» Electronic Visitor Management System		✓	✓	✓
» VMS-Assisted Background Checks				✓

STUDENT AND STAFF IDENTIFICATION

» Volunteer Background Checks	✓	✓	✓	✓
» Smart Card Identification Badges			✓	✓

• ARCHITECTURAL

» Facility and Vicinity Mapping	✓	✓	✓	✓
» Entrances Marked With First Responder Numbering System	✓	✓	✓	✓
» Printed or Electronic "Tactical Floor Plans"		✓	✓	✓
» Zone Emergency Response System			✓	✓
» Virtual Response Plans and Implementation				✓

• COMMUNICATION

» Wide-Area Two-Way Radio System	✓	✓	✓	✓
» Bi-Directional Amplifier (BDA) or Distributed Antenna Systems	✓	✓	✓	✓
» 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				✓

• ACCESS CONTROL

» Emergency Site Building Access System for First Responders	✓	✓	✓	✓
» Access Control System Equipped with Remote Door Release and Lockdown Capability			✓	✓
» Electronic Access Control for IDF & MDF Rooms w/Key Override				✓

TRANSPORTATION

» Interoperable Radio System for All Buses and School Vehicles	✓	✓	✓	✓
» Bus Video Surveillance/GPS System		✓	✓	✓
» Bus Video Surveillance System		✓	✓	✓
» Card-Based Check-In				✓

TIER 1	TIER 2	TIER 3	TIER 4
--------	--------	--------	--------



DISTRICT-WIDE LAYER (cont.)

• VIDEO SURVEILLANCE

» Incorporation of Video Surveillance Into Emergency Response Plans	✓	✓	✓	✓
» Camera Standardization		✓	✓	✓
» Recording System Standardization			✓	✓
» Video Verification of Intrusion Alarms to Monitoring Service, Administrators and/or SOC				✓
» Video Verification of Duress Alarms to a Monitoring Service, Administrators and/or SOC				✓

• DETECTION AND ALARMS

» ICentrally Monitored Intrusion and Duress Alarms	✓	✓	✓	✓
» Duress Alarms Sent to Law Enforcement		✓	✓	✓
» Graphical User Interface for Operators			✓	✓
» Intrusion and Duress Alarms Monitored by a District-Wide SOC				✓

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)¹⁹ 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)²⁰ 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),²¹ 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:

¹⁹ [fema.gov/plan](https://www.fema.gov/plan)

²⁰ [fema.gov/national-incident-management-system](https://www.fema.gov/national-incident-management-system)

²¹ [fema.gov/incident-command-system-resources](https://www.fema.gov/incident-command-system-resources)

The Five Phases of Emergency Management



1. **Prevention** focuses on training, hazard response plans and exercises ahead of an event to prepare through proactive planning. The risk of loss of life and injury can be limited through good evacuation plans, environmental planning and design standards.
2. **Mitigation** is the effort to reduce loss of life and property by developing structural and non-structural measures that will mitigate the effects of a disaster.
3. **Preparedness** is a continuous cycle of planning, organizing, training, equipping, exercising, evaluating and taking corrective action. These elements are the cornerstones of preparedness and focus on readiness to respond to all-hazards incidents and emergencies.
4. **Response** is the management of resources including personnel, equipment and supplies and utilizes the incident command system in an all-hazards approach. The response phase is a reaction to the occurrence of the event.
5. **Recovery** activities continue beyond the emergency period and focus on restoring critical functions to stabilize operations and increase capacity to continue to serve their community after a disaster. The goal of the recovery phase is to bring the affected areas back to some degree of normalcy as soon as possible.

TIER 1

A. 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.

B. 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

For further info see emergency procedures²² and guidelines from Safe and Sound Schools.

C. 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.

²² <https://safeandsoundschools.org/additional-resources-emergency-procedures-guidelines/>

D. 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

E. Pre-Approval of Applications for School-Issued Electronic Devices. Districts should ensure school-issued electronic devices only allow installation and use of pre-approved, authorized applications. This is becoming increasingly important due to growing concerns with cybersecurity risks associated with untrustworthy social media applications and others. Mobile application management software allows administrators to select all applications that can be installed on such devices, with user requests for additional application subject to approval.

F. 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 manufacturers offer training and certifications that technicians working with this equipment should obtain. At minimum, a yearly test should be conducted on all security technology implementations.

G. 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.

H. Conduct Lockdown Drills. Creating a safe environment so children and educators can focus on learning is the goal of school security and safety professionals. Drills and exercises are part of a comprehensive approach to ensuring a safe learning environment, and best practices should reflect this.

Drills are common in the school environment, whether in language or math education, sports practice or safety. Exercises are common to improve skills in specific areas or disciplines.

School safety drills and exercises are no different. To ensure a safe environment during the school day, common drills repeated during the school year are the accepted practice. For years, the standard “fire drill” practice has been to line up, exit the classroom single file and march to a safe rally area, such as the schoolyard.

The need for “lockdown” drills has grown due to the unique circumstances of the active shooter or assailant. Whether in a school, business or other public space, best practices now dictate having a lockdown protocol as the major component of an effective safety plan when escape is not possible. Other components may include methods to secure your area prior to sheltering notification and communication during an event.

In the school safety context, it is critical to distinguish between drills and exercises. Drills are educational opportunities to test processes, procedures and technologies. Exercises are mainly for first responders to test their training.

DESIGNING A DRILL

Lessons learned from decades of school fire drills may be employed here. What is an appropriate approach for schools to take as they plan, prepare and practice for protecting children and staff from danger that is inside the building?

Start with standardizing the term by calling these drills “lockdown” drills, as called for by the National Association of School Resources Officers (NASRO) and National Association of School Psychologists (NASP), and not “active shooter” drills or “active assailant” drills. PASS supports NASRO and NASP’s position on designing drills. A lockdown should be looked at as an active threat situation, or a situation that presents an immediate and ongoing danger to the safety of students, staff and visitors. In addition to individuals using firearms (active shooters), other types of weapons and erratic behavior can also create active threat (lockdown) situations. These are matters of urgent concern not only to schools, but also to other public spaces nationwide.

A NOTE OF CAUTION WHEN DESIGNING DRILLS

Some have called for making these drills realistic; however, schools are not set on fire to practice fire drills. Firefighters do not run through the building yelling at students and staff during fire drills. Firefighters use practice “exercises” to train in fighting fires. Schools have “drills” to educate/train students on how to evacuate the building in the event of a fire. Drills should be conducted in an educational way—there is no need for violent simulations.

WHAT SHOULD BE TAUGHT IN A DRILL?

Both staff and students should be educated about the options that can be used in an active threat situation. Realistically, students and staff are not always in their classrooms or behind closed doors as they go throughout their busy school days; because of this, students and staff should be taught additional strategies that go beyond just sheltering in a classroom. For example, there are other shelter options that should be taught, like what a staff member or student should do when in a bathroom, cafeteria, or hallway if an active threat arises. This is where evacuation (evade) or distraction (defend) strategies could come into play. Another critical option that staff and students can be educated on is care, which could be first aid or just being helpful to others in these situations.

When a lockdown drill occurs at an elementary school, it should be conducted when the majority of the school is sheltered inside and when some classes are outside at recess. The staff and students at recess could practice how to safely leave the school grounds to seek safety. Students in a secondary school can be taught what to do if they are caught in different locations inside and outside the school. Those at recess need to know what their options are outside the building, and they should be guided through the options. Age-appropriate strategies can also be offered as classroom lessons, wherein students are told about the different options that they may consider in an active threat situation.

Additional training, such as basic first aid, should also be considered when creating a lockdown drill. Many local emergency medical responders, the Red Cross and other organizations can provide age-appropriate training for students and staff.

8 PASS Recommendations for Conducting School Safety Drills

- 1. Purpose:** Drills should be conducted in a way that is educational and involves the practice and testing of established processes, procedures and technologies. They should not involve violent simulations that could be traumatizing to participants.
- 2. Scheduling:** Drills should be announced to staff, students and parents and include a scheduled time frame in which the drill will be conducted (e.g., Monday between 9 a.m. and noon). Drills should not be conducted in a “surprise” fashion.
- 3. Duration:** Drills should be short and conducted as quickly and efficiently as possible.
- 4. Times and locations:** Drills should be conducted at varying times throughout the school day—recess, passing periods and lunch time—and during after-hours activities such as child care and athletics.
- 5. Evaluation:** Staff should be debriefed immediately following a drill where feedback can be exchanged. Drills should be run for other groups such as after-school child care and athletics.
- 6. Frequency:** At least two lockdown drills should be conducted each school year. It is recommended to practice within the first 20 days of the start of the school year and within the first 20 days after winter break.
- 7. Drills vs. exercises:** Any participants selected for “exercises” should be volunteers and be carefully selected, given the significant difference between a drill and an exercise. Drills involve all or most occupants of a school facility to test processes, procedures and technologies. Exercises are mainly for first responders to test their training.
- 8. Safety awareness levels:** Drill design should be tailored to desired levels of safety awareness, which will vary depending on the developmental levels of students and the capabilities and training of staff involved. PASS recommends referring to Safe and Sound Schools’ Developmental Levels of Safety Awareness resource to help guide this process.

TIER 4

A. Independent Security Assessment on 3-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 (VMS) 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. 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. This usually involves checking the ID against the National Sex Offender Database, but can also involve 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.

ID Scanning Technology—A Key Element of VMS.

At this time there are two primary scanning methods used by the industry which are 2D barcode scanning and optical character recognition (OCR). 2D barcoding offers the advantages of being less prone to misreading errors and the photo and scanning equipment tends to be less expensive. The OCR advantage is that the reading process happens in a single step. Generally, both processes should not take more than 30 seconds.

PASS recommends that visitor management systems utilize the National Sex Offender registry (<https://www.nsopw.gov/>). A prohibited person registry is a capability that your visitor management system should offer. Prohibited person registries are generally maintained by the school district and include information on people issues, like ‘no trespass’ orders, domestic situations and other flagged persons.

PASS recommends when implementing a visitor management system that good policies and procedures are developed. Policy and procedures should address the alert notification process on when a positive hit is received. This should address the sending of alerts if a visitor appears to be on the sex offender registry, but how to verify (by photo) if the visitor and sex offender are the same person; how to handle “false” positives and how to include comments about the visitor for future handling at the campus or other campuses in the district.

PASS recommends that when a visitor management system is installed that it be monitored district wide as well. When a visitor enters a school, your front office staff should be able to see where they have been in the district and if appropriate, add notes that can be viewed by staff at other campuses. It is valuable to have a one-button report of everyone on campus in case of emergencies, but it can also be beneficial to see everywhere a visitor has been throughout the school year. If your district has a security operations center they can help monitor this global process and clear positive and false positive matches.

TIER 4

- A. VMS-assisted Background Checks.** The higher-tier VMS implementation provides the capability to run criminal background checks for all volunteers. This feature is typically done through a pre-enrollment process. Potential volunteers will pre-enroll through a web link set up by the district and provided by the visitor management company. As recommended in Tier 3, it is important for a district to have good policy and procedures in place that shows how a district will deal with someone with a record, what convictions limit a person from serving as a volunteer and who has the authority to decide whether a visitor will or will not be restricted from entering one or all schools. It is very common for a visitor management system to also report criminal records that have been sealed. Policies should be developed to address that scenario as well.

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.

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 the 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.

ARCHITECTURAL COMPONENT:

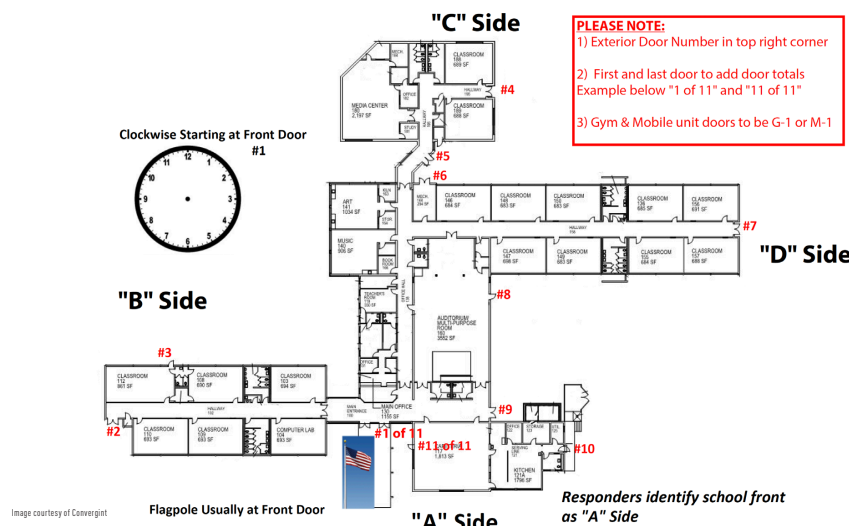
TIER 1

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:

- Location of the rapid access security vault (RASV), a secure storage device where access credentials (keys, cards) are kept for emergency access.
- Printed or electronic copy of "As-Built/Record Drawing" of facility. Plans should include all room names and associated numbers.
- 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.

B. Entrances Marked with First Responder Numbering System. All entry doors should be clearly marked with a first responder door numbering system, 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. The number system should be clear to the first responder as to where the door is within the relation to the layout of the school. While door numbering conventions in use share many similarities, PASS recommends adoption of the following convention (see figure) for greater consistency nationwide, which has been adopted by the Georgia Department of Education and is under consideration by NFPA in its 2022 update of the ASHER national standard. This is similar to the convention used by the Center for Safe Schools in Pennsylvania, the New Hampshire Department of Safety and others, where labeling begins at the main entrance and proceeds clockwise around the building.



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. Zone Emergency Response System. A zone emergency response system is an improved emergency response system and method for use in responding to emergencies and reducing the time it takes to get responders to the right location in a building or campus. An emergency dispatcher, or electronic equivalent, can reference designated directional zones to relay important directional information regarding a target location to first responders, regardless of whether additional premises-related information is immediately available. In addition, the zones can be displayed in a superimposed manner relative to mapped features of the local premises, such as satellite photos, site maps, architectural plans, etc.

TIER 4

A. Virtual Response Plans and Implementation. There are a number of products and resources available to create 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. 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 System²³ must be used, not off-the-shelf consumer products or radios designed for recreational use.
- B. Bi-Directional Amplifier (BDA) or Distributed Antenna Systems (DAS).** These technologies boost reception in and around buildings for emergency personnel radio networks on 700 MHz, 800 MHz and 900 MHz bands, as well as mobile phones and other devices if needed, where it would otherwise be inconsistent or unavailable due to surrounding construction materials or other factors. BDA systems use special cabling and boost all carrier networks, while distributed antenna systems use a series of antennas and typically cover larger areas for a single carrier network. Hybrid systems that combine these elements are also being implemented. PASS recommends consulting with a radio systems integrator and contacting both local law enforcement and fire departments that may have either a standard for such technologies or require the appropriate NFPA code, to coordinate the best plan to implement these technologies throughout a district.

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.

²³ For license example, see wireless2.fcc.gov/UlsApp/ApplicationSearch/appMain.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 feed²⁴ 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 lightning and tornados. Site-specific warning technology typically includes lightning proximity and all-clear notifications that can help protect students and staff participation in outdoor events.

TIER 4

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. 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.

²⁴ 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 the property, parking lot and 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 access to specific openings at specific times. Emergency access through an RASV should be provided at multiple locations around the building, or at property and parking lot perimeters if secured, to ensure rapid access. Districts should provide access credentials to the RASV to all emergency responders.

TIER 1

A. Emergency Site Building Access System for First Responders. Mechanical keys or cards should be available to district and community emergency responders for all mechanically or electronically controlled openings to provide an emergency override. Access credentials and other necessary keys should be placed in a KNOX box or other Rapid Access System (RAS) in use locally. While emergency access is critical, access to keys and cards should be tightly controlled and limited to key personnel and first responders.

TIER 3

A. Access Control System Equipped with Remote Door Release and Lockdown Capability. The control of an access system through a remote connection allows designated school personnel to open or lock any door that is part of an electronic access control system. This remote capability can typically be accomplished via an access control system smartphone app, a laptop connection to the school network, and designated computers at a dispatch or emergency operations center, and also provides emergency entry by law enforcement or other first responders. Additionally, schools should consider establishing system access rights that limits these capabilities only to those staff members responsible for responding to emergencies (SROs, safety personnel, and designated administrators).

TIER 4

A. 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).

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 for 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).

TIER 2

A. Bus Video Surveillance/GPS System. School bus surveillance systems provide an increasing number of safety and security benefits. Increases in both capability and affordability have led many districts to implement this technology. A typical school bus camera system consists of two to eight specialized mobile cameras and a mobile digital video recorder for each vehicle, with GPS. 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 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. GPS tracking allows a school district to know where buses and school vehicles are in real time, as well as possible integration with check-in system. GPS features 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) when connectivity or power is available intermittently and real-time data is not required.

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 at 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.

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 through 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.

A. 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 enroute 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 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 Intrusion Alarms to Monitoring Service, Administrators and/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.

B. Video Verification of Duress Alarms to a Monitoring Service, Administrators and/or SOC: An emergency duress system should be integrated with the existing camera system and video available to designated response personnel. Live video access is critical because it provides real-time intelligence for first responders and other staff members responsible for emergency coordination and support. 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. Centrally Monitored Intrusion and Duress Alarms. 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.

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

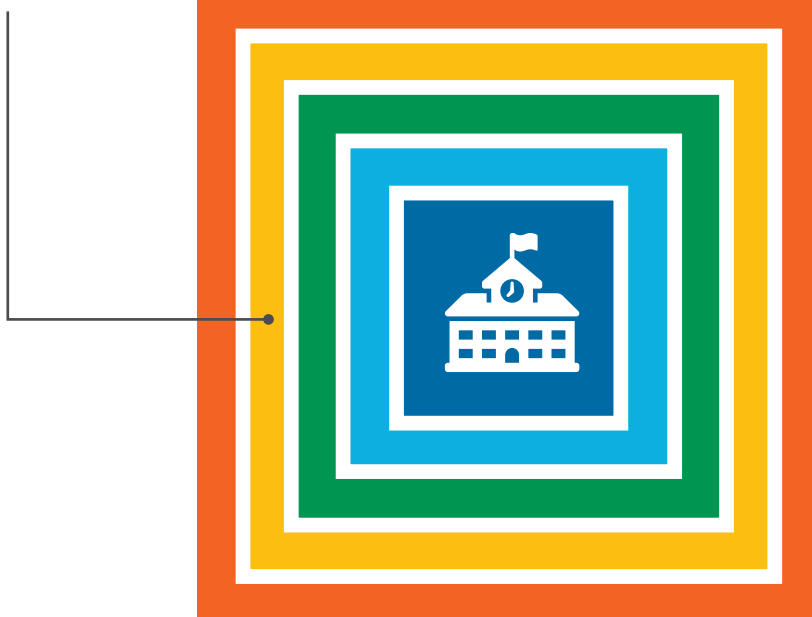
A. Graphical User Interface for Operators. School districts should consider providing graphical maps and interfaces that allow users to interact with and monitor unified security system technology in real time. Many school districts utilize a digitized map of a school that displays where the security devices are laid out in their exact locations. Information from camera feeds, card readers and other devices can be easily accessed and monitored in such a manner. For example, motion detectors, latch position and door contacts can be indicated on the map to change color when a change is detected. This real-time information provides staff with instant situational awareness during emergencies.

TIER 4

A. 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. The advantage of having a SOC is that a district can use 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.



PROPERTY PERIMETER LAYER



» QUICKFIND

Property Perimeter Best Practices	42
Policies and Procedures Component	43
Architectural Component	44
Communication Component	45
Video Surveillance Component	46



PROPERTY PERIMETER LAYER

	TIER 1	TIER 2	TIER 3	TIER 4
• POLICIES AND PROCEDURES				
» Implement NCS4 Best Practices for Outdoor Activities and Events	✓	✓	✓	✓
» Annual Assessment of Safety of Ground (including Lighting) (new for 5th Edition)	✓	✓	✓	✓
» Create Grounds and Facility Use Policies for Outside and Public Groups (new for 5th Edition)	✓	✓	✓	✓
» 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			✓	✓
» Install Audio/Video Call Boxes at Key Locations (new for 5th Edition)				✓
» 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	✓	✓	✓	✓
» Infrared (IR) Cameras or Lighting		✓	✓	✓
» Wireless Video Data Transmission		✓	✓	✓
» PTZ Camera Coverage		✓	✓	✓
» Loitering Detection Analytics		✓	✓	✓
» Perimeter Video Analytics				✓

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 guide²⁵ 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.

B. Annual Assessment of Safety of Ground (Including Lighting). An ongoing process should be established for identifying, evaluating and prioritizing risks and areas of weakness within the property perimeter that could have adverse consequences for individual schools and school districts. This can be done by conducting a walk-through of school grounds and facilities and looking at existing crime and school incidence data. The goal should be to design a system of accountability with measurable activities and timelines to address risks that were found. Self-assessments are appropriate and should be done by various district stakeholders that oversee the exterior areas of the facility.

C. Create Grounds and Facility Use Policies for Outside and Public Groups. Such policies not only protect schools but also promote the facilities as assets to the community in many ways. While buildings and grounds are maintained primarily for the purpose of educating students, most school boards recognize that district facilities are a valuable community resource and believe they should be made available to the community for beneficial uses that will not interfere with educational activities or disrupt district operations such as renovation, maintenance and/or sanctioned after school activities.

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.

²⁵ 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 for Territorial Reinforcement, Access Control and Natural Surveillance. 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. For new construction, landscaping should be planned with clear sight lines in mind. It is also recommended to establish clear sight lines from perimeter windows to the parking lot by removing or trimming vegetation. 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. 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 candle²⁶ 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.

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.

²⁶ 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.

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 with the district and local emergency responders as needed by simply changing the frequency on the radio.

TIER 4

A. Install Audio/Video Call Boxes at Key Locations. Audio and video emergency call boxes have been popular and effective technology deployments for maintaining safe school campuses. While more prevalent on college campuses, many K-12 schools are also realizing the benefits of utilizing video call boxes for emergency situations, and in some cases for access control. These same call boxes can also be configured to work on a 24/7 basis beyond access control where someone utilizing the grounds who may be in trouble could access the call box to call for help.

B. 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.

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.

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 as 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.

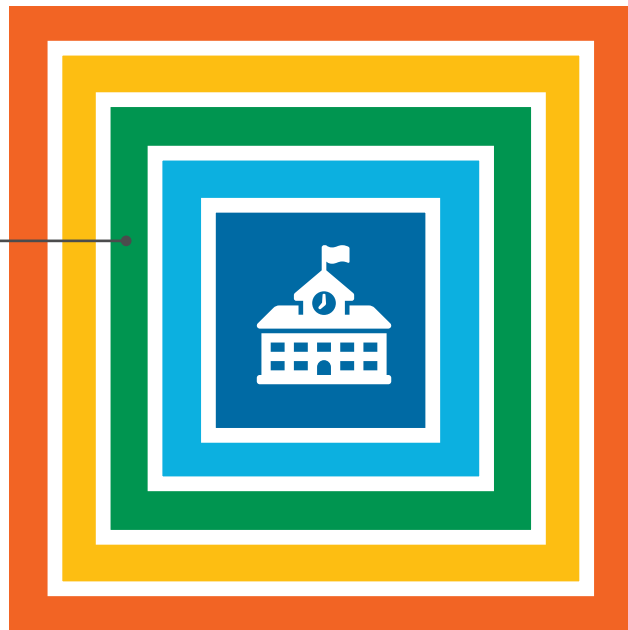
PTZ cameras should be rated for outdoor use to prevent ingress of dust or water and environmentally rated to function in both upper and lower temperature ranges. They should also include wide dynamic range sensors to ensure image usability.

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.

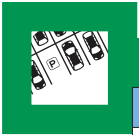


PARKING LOT PERIMETER LAYER



» QUICKFIND

Parking Lot Perimeter Best Practices	50
Policies and Procedures Component	51
Architectural Component	52
Communication Component	52
Video Surveillance Component	53



PARKING LOT PERIMETER LAYER

	TIER 1	TIER 2	TIER 3	TIER 4
• POLICIES AND PROCEDURES				
» Parking Tags	✓	✓	✓	✓
» Assign Staff to Periodically Check Parking Lot		✓	✓	✓
» Persistent Staff Patrol			✓	✓
» RFID Parking Tags			✓	✓
» Staff Capability to Initiate Emergency Protocols From Exterior				✓
• ARCHITECTURAL				
» Signage (Directing to Appropriate Areas)	✓	✓	✓	✓
» Signage Directing to Emergency Communication Device	✓	✓	✓	✓
• COMMUNICATION				
» Wide Area Mass Notification System (MNS)			✓	✓
» Two-Way Emergency Phones			✓	✓
» Install Audio/Video Call Boxes at Key Locations (new for 5th Edition)				✓
» 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	✓	✓	✓	✓
» People Identification Field of View at Pickup/Drop-off Area		✓	✓	✓
» PTZ Camera Coverage			✓	✓

POLICIES AND PROCEDURES COMPONENT:

TIER 1

- A. **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, including 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. 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.
- B. 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 Notification 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 provide districts with 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. Install Audio/Video Call Boxes at Key Locations.** Audio and video emergency call boxes have been popular and effective technology deployments for maintaining safe school campuses. While more prevalent on college campuses, many K-12 schools are also realizing the benefits of utilizing video call boxes for emergency situations, and in some cases for access control. These same call boxes can also be configured to work on a 24/7 basis beyond access control where someone utilizing the grounds who may be in trouble could access the call box to call for help. Some school districts are now deploying the same call boxes colleges utilize in parking lots and other highly visible and accessible locations on school grounds.
- B. 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.

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 in 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. Wide dynamic range 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.

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.

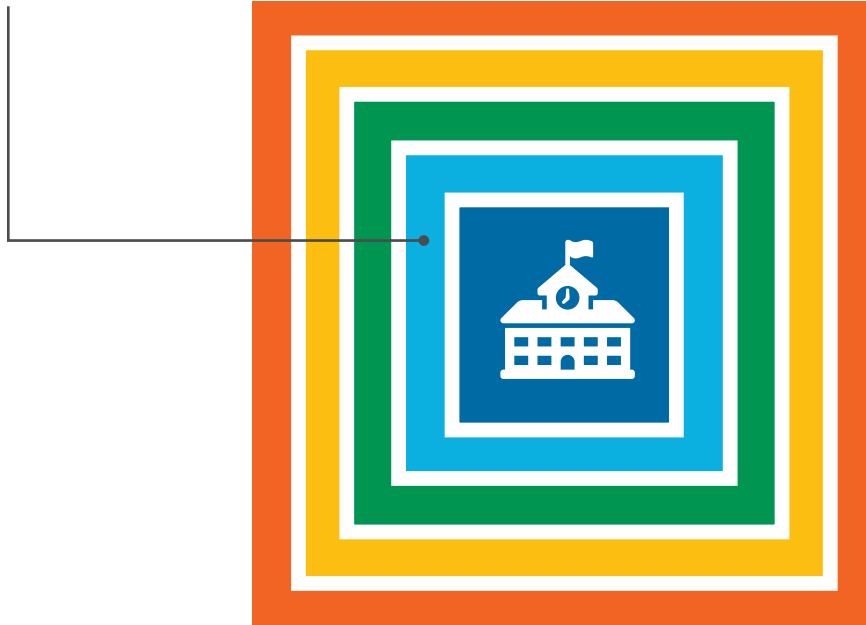
TIER 3

A. 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.



BUILDING PERIMETER LAYER



» QUICKFIND

Building Perimeter Best Practices	56
Policies and Procedures Component	57
People (Roles and Training) Component	58
Architectural Component	58
Communication Component	59
Access Control Component	66
Video Surveillance Component	61
Detection and Alarms Component	63



BUILDING PERIMETER LAYER

	TIER 1	TIER 2	TIER 3	TIER 4
• POLICIES AND PROCEDURES				
» Categorization of All Exterior Openings	✓	✓	✓	✓
» Policy Established for Control of Exterior Openings	✓	✓	✓	✓
» Key Control Procedures	✓	✓	✓	✓
» Complete BDA/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)	✓	✓	✓	✓
» Secured Vestibule	✓	✓	✓	✓
» BS/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 (Door Position and Latchbolt Position)	✓	✓	✓	✓
» Electronic Access Control of Primary Entrances	✓	✓	✓	✓
• VIDEO SURVEILLANCE				
» Video Intercom at Visitor Entrance Points	✓	✓	✓	✓
» Interior, Fixed Camera Coverage for All Entrance Points	✓	✓	✓	✓
» Exterior, Fixed Camera Coverage at All Entry Points		✓	✓	✓
• DETECTION AND ALARMS				
» Intrusion Detection System on all Exterior Access Points	✓	✓	✓	✓
» Intrusion Detection System Monitored 24/7	✓	✓	✓	✓
» Partitioned Intrusion Detection			✓	✓

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 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. 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.
- C. 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.
- D. Complete BDA/DAS Site Survey.** Bi-Directional Amplifier (BDA) and Distributed Antenna Systems (DAS) 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.

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. 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).
- C. BDA/DAS System (New Construction/Renovation).** Two-way radio signal boosters may be required in new construction/renovation for compliance with the emergency responder radio coverage. Requirements are determined 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 these technologies through IFC-510 or NFPA-72, Chapter 24.
- D. 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.
- E. Security Film for Exterior Door Vision Panels and Sidelites.** Security window film at least 14 mils²⁷ thick (350 microns) should be installed on all exterior door vision panels²⁸ and sidelites.²⁹ 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

²⁷ Updated August 2023 from millimeters to mils.

²⁸ Door vision panels are windows incorporated into a door.

²⁹ Sidelites are narrow windows immediately adjacent to a doorway.

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.

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 students 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 to the students and staff through 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 to indicate whether the door is open or closed. This is typically done with a door position switch, which is either wired or wireless, and monitored centrally and remotely through a facility's access control system. Additionally, the "latchbolt" of the door can be monitored to see if the door is locked, in addition to being closed. Latchbolt monitoring, along with monitoring the door status (open/closed), provides the most effective way to ensure exterior doors are both closed and secure from the outside.
- 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 in 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

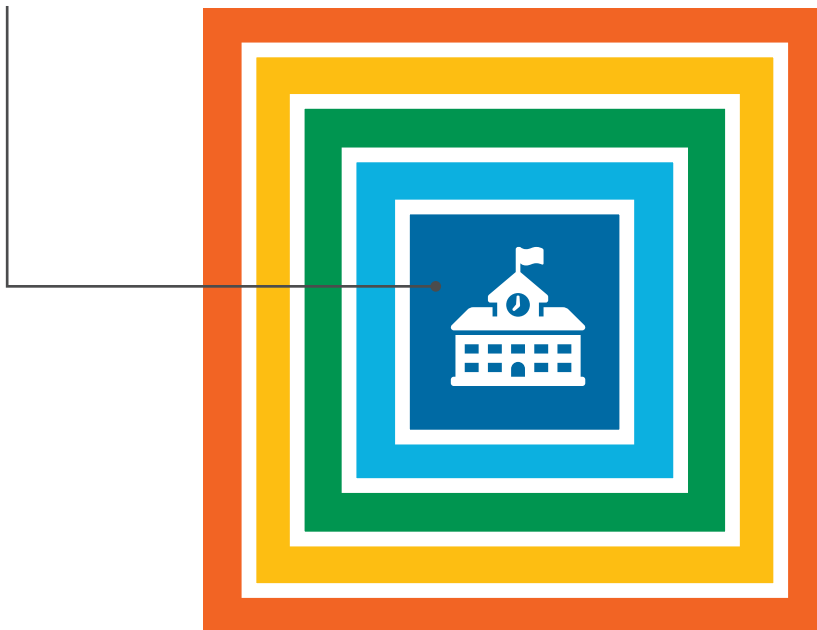
It is preferable to mount cameras facing the door to record people entering the building to ensure schools have a visual record of someone entering (at a quality level allowing for identification), as the other cameras inside the building and outside the entrance, in many cases, can be used to determine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

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 in 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.



CLASSROOM/INTERIOR PERIMETER LAYER



» QUICKFIND

DETECTION AND ALARMS COMPONENT:

TIER 1

- A. Intrusion Detection System on All Exterior Access Points. If a school is



CLASSROOM/INTERIOR PERIMETER LAYER

	TIER 1	TIER 2	TIER 3	TIER 4
• POLICIES AND PROCEDURES				
» Classroom Doors Closed and Locked When Occupied	✓	✓	✓	✓
» Designate Shelter Areas Outside Corridor Line of Sight (new in 5th Edition)	✓	✓	✓	✓
• 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)	✓	✓	✓	✓
» Local Area Two-Way Radio System for Select Staff	✓	✓	✓	✓
» Two-way Intercom System with Call Buttons		✓	✓	✓
» Duress Button System - Office and Classroom		✓	✓	✓
» Local Area Two-Way Radio System for All Staff, Including Teachers		✓	✓	✓
» In-Building Emergency Communication System			✓	✓
» BDA/DAS System			✓	✓
» 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				
» Classroom and Shelter in Place Doors Equipped with Office/Entry, or Classroom Security Function Locks	✓	✓	✓	✓
» Locks with Visual Indicator		✓	✓	✓
» 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		✓	✓	✓
• 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				✓

not equipped with an access control system that can monitor whether each exterior door is open or closed, PASS recommends an intrusion detection system that uses door position switches to monitor the status of doors.

- 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.

Classroom/Interior Perimeter Best Practices.....65
Policies and Procedures Component66
People (Roles and Training) Component67
Communication Component68
Access Control Component72
Video Surveillance Component74
Detection and Alarms Component75

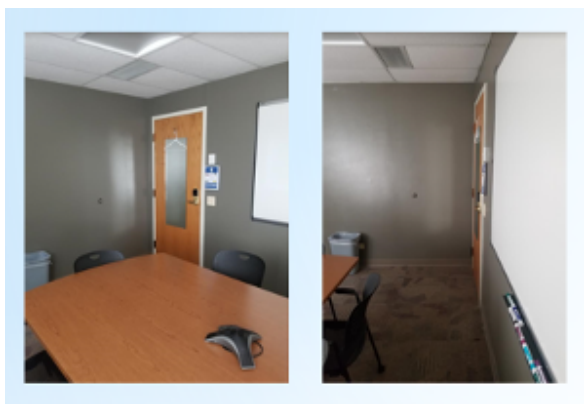
The most important assets to protect in a classroom (and on school grounds, for that matter) are students, staff, faculty and visitors. The security components within outer layers detailed in this guide also serve to protect classrooms and other interior areas of a school facility. These best practices 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:

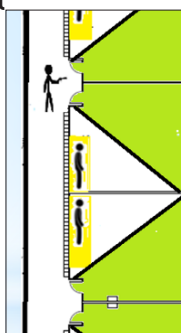
TIER 1

- 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.
- B. **Designate Shelter Areas Outside Corridor Line of Sight.** Each classroom should have a pre-identified area in which the occupants could shelter out of the line of sight from the entry door during an emergency. This could be a nook in the room layout or simply a “hard corner.” This location in each classroom should be clearly identified to both staff and students using the classroom.

View from Room Center View from “Hard Corner”



Green Areas Viewable Through Door Vision Panel



PEOPLE (ROLES AND TRAINING) COMPONENT:

TIER 1

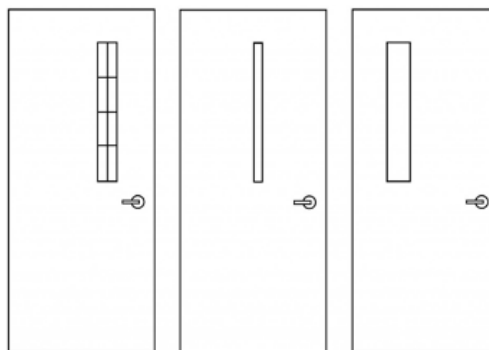
- A. Teachers, Staff and Substitutes Trained on Emergency Protocols.** Teachers and supervising staff have several important responsibilities before and during an emergency. Students will count on teachers and supervising staff to provide direction. The actions of teachers and supervising staff are integral 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 mils³⁰ thick (350 microns) should be installed on all classroom and shelter in place room door vision panels³¹ and sidelites.³² 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. Installation is typically performed by an authorized installer, and they must follow the manufacturer's recommended procedures in order for these products to be effective.
- 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.



³⁰ Updated August 2023 from millimeters to mils.

³¹ Door vision panels are windows incorporated into a door.

³² Sidelites are narrow windows immediately adjacent to a doorway.

- 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.

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.³³ 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.³⁴ 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.³⁵

³³ Relevant standards include National Electrical Manufacturers Association SB-40, Communications Systems for Life Safety in Schools.

³⁴ “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.

³⁵ For license example, see <http://wireless2.fcc.gov/UttsApp/ApplicationSearch/appMain.jsp?appID=9075468>.

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.

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 speakers³⁶ 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.

³⁶ Relevant standards include UL 2017, Standard for General-Purpose Signaling Devices and Systems.

- B. BDA/DAS System.** 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 BDA/DAS explanation in the district-wide layer). These technologies can incorporate boosters for two-way radios and cellular and are typically custom designed for each unique environment.
- C. Mass Notification Tied to District-Wide System.** As described 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.
- **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 receive the highest implementation priority.

One well-known study³⁷ 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.

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?

37 "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



A Key to Safe Classrooms

According to industry best practices, locks on classroom doors should meet the following parameters:

- Classroom locks should be easy to lock and allow for quick release in the event of an emergency.^{1,5}
- All doors should be lockable from inside the room without opening the door.^{1,2,3,4}
- Locks on classroom doors should be able to open from outside of the room with key or card, allowing access for administration or law enforcement.^{4, model codes}
- Classroom locking devices should comply with fire, life safety and ADA codes and requirements.^{1, 4}
- Keys or credentials should be always in the possession of teachers and staff.^{2, 3}

¹ Sandy Hook Incident Report, "Key Safe School Infrastructure Standards", page 73, Exterior Doors | ² Marjory Stoneman Douglas High School Public Safety Commission, 01/02/2019 | ³ Investigative Committee on the Robb Elementary Shooting, Texas House of Representatives, Interim Report July 17, 2022 | ⁴ Final Report of the Federal Commission on School Safety, 12/18/2018

Recommended Lock Function for Classrooms

Classroom Security Function Lock

With this function, a key on either the inside or the outside will lock the outside lever ONLY.

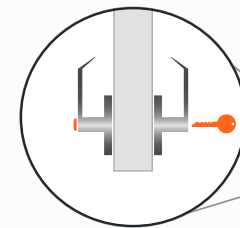
The inside lever remains unlocked at all times, allowing students and teachers to exit at any time.

Pros:

- The door is able to be locked from the inside during a lockdown, reducing risk.
- Key control keeps unauthorized people from locking the door.

Cons:

- Key must be present, and may need to be located and used in high-stress situations.



Office/Entry Function Lock

In addition to a keyed outside lever, a thumb turn or push button on the inside can lock or unlock the outside lever.

Pros:

- The door is able to easily be locked from the inside during a lockdown.
- A key holder does not need to be present to lock the door, eliminating the need to issue keys to substitute teachers.

Cons:

- Anyone inside of the room can easily lock the door, creating opportunity for student-led violence or mischief.

Electronic Locks

When used on classroom doors and tied into a centralized access control system, electronic locks provide the following increased security benefits:

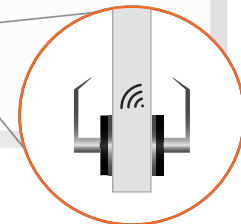
- All connected doors lock down in seconds with the push of one centralized button
- Instant notifications can be sent to office or SRO alerting others a lock down has been initiated.
- Real-time status displaying whether the door is closed, latched and/or locked.
- Eliminate the need to issue substitute teachers a key to lock down the classroom.
- Card technology allows instant management of who and where cards can be used, eliminating the risk of lost keys.

Pros:

- All rooms are immediately locked down without a key.
- No one has to go to a door and lock it in an emergency.
- No keys required, so key holder does not need to be present to secure the room.

Cons:

- Solution leverages latest technology, providing a higher level of security, but also incurring a higher level of initial cost.



- 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 (and other shelter in place 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.³⁸
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 be possible from the inside of the room.³⁹
4. Locks should ideally have a visual indicator so that the condition of the lock (locked or unlocked) is visible to room occupants.

Some manufacturers offer code-compliant conversion or retrofit kits which are capable of converting existing locks to comply with the above criteria.

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 Americans with Disabilities Act (ADA). PASS recommends that school administrators work with local life safety experts to determine code compliance related to securing classroom/interior doors.

TIER 1

A. Classroom and Shelter in Place Doors Equipped with Office/Entry or Classroom Security Function Locks. All classrooms *must* have the ability to be locked from the inside by means of “Office/Entry” or “Classroom Security” function locks (or electronic locks in higher tiers – see infographic below). This is critical as many classroom doors in use today do not meet these criteria. As schools transition to this ability, they should also place an emphasis on clarifying human roles and communicating processes to staff that are essential to effective use of the hardware that is chosen.

The choice of which type of lock to use involves tradeoffs and should consider the room’s normal occupants and intended use, a facility assessment and any relevant state laws or local requirements.⁴⁰ As noted above, all classroom doors should lock from the inside and be keyed or otherwise accessible on the corridor side for quick access by authorized personnel.

PASS does not recommend any use of magnetic strips or other devices that impede the ability of a door to lock. Holding the device in an unlocked state contrary to its design could impact the long-term dependability of the lock mechanism to engage.

³⁸ 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.

³⁹ 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

⁴⁰ Some states require a specific type of lockset among these for classrooms; for more information, see idighardware.com/schools. Some states require a specific type of lockset among these for classrooms; for more information, see idighardware.com/schools.

TIER 2

A. Locks with Visual Indicator. Classroom locks that provide a visual indicator allow the condition of the lock (locked or unlocked) to be visible to staff and room occupants, without them having to exit the room to check.

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 and provide keyed or credential access on the corridor side for quick 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. Some locks have the ability to be programmed to 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.

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

- A. 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.
- B. 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 but also allows for processes to be implemented at other facilities, based on the threat detected.
- C. 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.

Enhanced Technologies

Beyond the safety and security components PASS recommends on the Tier Continuum, schools may want to consider enhanced technologies that show potential for making significant improvements to school safety but may not yet be widely adopted. Below are just a few of these technologies that have received significant recent interest, as well as their potential benefits.

The Pilot Program

A pilot project is a good way for districts to evaluate new security products, particularly enhanced technologies, prior to full-scale implementation. This allows the collection of data on its performance, refinement of processes and even finding additional beneficial uses. Many manufactures and integrators will provide products and services that can be tested by end users in a small, controlled location before they are deployed on a larger scale. PASS encourages end users “to try before you buy” when it comes to enhanced technologies to ensure that the technology or service will work with your district security posture and systems.

The Goal: Unified Security and Life Safety Systems

Any enhanced technology implementation should further the unification of security and safety components and related systems by school districts. Unified systems address the difficulties of integrating technologies across different platforms and within the connected environment in which they reside. Properly implemented, a unified system eases integration of new components and allows a district to continue to evolve and expand. It is important for a school district to work with their integrator to ensure facility infrastructure can support any new technology as part of a unified system.

Weapons and Prohibited Items Detection

The need for weapons and prohibited items detection systems will vary across schools and districts based on physical layout and risk profile. While such technologies alone cannot prevent all weapons from entering schools, they can provide an additional and critical layer of safety and security for students, staff and visitors, when procured and utilized as designed. Modern detection technologies could play a key role in averting or mitigating attacks. According to a 2021 U.S. Secret Service analysis of plots against schools from 2006-2018, over half the plotters in 67 averted attacks (n=37, 55%) chose to use at least two or three types of weapons, and in nearly all of the cases (n=64, 96%) the weapon(s) of choice were firearms, versus incendiary devices or knives (which are more difficult to detect). The “human factor” is critical. Implementation should support clearly communicated district-wide policies on what is permitted on campus and should be accompanied by clear procedures and staff training regarding the response when a prohibited item or threat is detected.

Metal detectors. Traditionally, detection has been carried out through use of walk-through metal detectors (WTMDs) or hand-held metal detectors (HHMD), often with the latter as secondary screening. This will be most effective when the number of entry points to a building or sporting fields for events, etc. are limited to one or as few as possible. If a person transiting the WTMD triggers an alarm, they are quickly moved aside where security uses a HHMD to pinpoint the object in question without having to physically touch them. WTMDs combined with HHMDs provide a faster, more accurate and less intrusive than hand-held screening alone resulting in an overall better experience for students and staff. With HHMD alone, screening consistency and accuracy can vary

among individual screeners.

Passive detection. Several technologies are becoming available that allow contraband and weapons detection without intrusive or labor-intensive screening—with the potential for tremendous positive impact on school safety. For example, terahertz and millimeter wave technology can detect a wide range of both metal and nonmetal items through a variety of materials and from a distance. Additionally, advanced image analysis in conjunction with video surveillance systems has been increasingly leveraged for weapons detection.

Vape Detectors

Vaping is not only a significant health risk to children, it has also become an enormous behavioral issue within many schools as it is very difficult to detect. Vape detection technology is now available that utilizes sensors resembling smoke or carbon monoxide detectors. These devices can detect vaping in places such as bathrooms or confined areas. Currently most of the providers of vape detectors offer a service that will send a text notification to designated staff when there is a detection of vaping in the vicinity of one of the sensors. An effective best practice in conjunction with vape detectors is ensuring that there is camera coverage of the hallways outside of restrooms or entrances where this activity commonly occurs. When a detection is made, the time of the vape detection and images of entry and exit into the space can be compared. Sensors should be hardened against vandalism and deployment should be accompanied by other procedures to counter efforts to defeat or disable them, such as sealing or alarming any restroom windows.

Electronic Hall Passes

The use of electronic hall pass systems in concert with detection technologies is an approach that can help further reduce student vaping, in addition to many other benefits. These systems typically allow students to use electronic devices to submit requests for hall passes more freely and conveniently. When a request is submitted electronically, the teacher can quickly approve or deny the request with less classroom disruption and more time on tasks. Other authorized staff can see that the pass has been issued on their devices, which makes it easier for them to tell if a student they encounter during instructional periods has a valid hall pass and is in a location consistent with the pass.

These systems can help prevent vandalism, truancy, sexual misconduct, fights and other problem behaviors, by displaying and controlling which students have passes at specific times. One example is being able to enforce “no contact” orders related to harassment or stalking. Administrators can enter the names of students who are not supposed to have contact with each other, so the system will not approve requests from either student if the other student is out of class with a pass.

Enhanced Data Analytics for Threat Detection

Beyond video analytics capabilities routinely included in video management systems, there are other enhanced data analytics capabilities that districts may consider adding, depending on their needs. **Audio analytics** involves the use of sensors and software that can detect and identify specific acoustic signatures of threat indicators, such as glass breaking, gunshots, aggression or panic in people’s voices and audible alarms. This technology can be loaded directly on cameras (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. 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. There are additional types of sensors as well for **gunshot detection**

that would provide similar alerts, including those based on technology to detect specific shockwave, infrared or smoke signatures from firearms discharge.

In more frequent events, speeding is a major factor in a large proportion of crashes, injuries and fatalities on school grounds. Some video management systems have **speeding vehicle analytics**. The systems can be helpful in detecting dangerous driving behaviors of students, especially in high school parking lots. Additionally, License plate reader (LPR) and data 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 if a related vehicle enters the property. Implementation of any of these technologies should follow manufacturer guidelines for sensor selection and placement.

Biometrics

Biometrics are the measurement and matching of physical characteristics unique to an individual, which provides an accurate way to authenticate identity that is often more efficient and secure than other methods. Use of biometric technologies in K-12 schools is becoming more prevalent as they become widely deployed in the private sector to improve business practices and secure financial transactions. While the primary rationale for use of biometrics by a school or district is to streamline administrative functions requiring identity verification and enhance data security (such as account access), there are physical security applications as well.

Finger scanning technology offers a good example of how biometric authentication technology can enhance operations without compromising privacy. During electronic enrollment of the biometric, a staff member or student's fingerprint is translated to a numerical format based on features of the finger lines, creating a unique code that is then associated with the person's identity in a school database. The fingerprint itself is not recorded—only the unique code issued by the specific software used 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 compare the codes, making it nearly impossible for data to be used outside the system and beyond the purpose for which it was created. Use of biometrics should be governed by a use policy set at the district level, include requirements such as providing a parental opt-out procedure to ensure any student participation is voluntary, and ensuring the destruction of all biometric-related information associated with a student or employee when they end their association with a school.

Biometric readers can reduce or eliminate the need for (and expense of) using cards and keys or remembering PINs and account numbers. Biometrics-based check-in for transportation pick up/drop off for example, works the same 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. Keys and cards do not identify the person holding them, and thus are more vulnerable to use by unauthorized persons.

Facial Recognition. While biometric technologies like finger scanning have been used for many years in K-12, the emergence of facial recognition offers some advantages by allowing a touchless interface and requiring less complex technology, using digital images for account enrollment and verification. It also offers other promising benefits for enhancing security systems and procedures.

There are numerous school districts in the U.S. successfully deploying facial recognition technology for the narrow purpose of checking individuals entering school property against a small list of enrolled images maintained by the district, providing notification to school staff when there is a potential match. Such images are typically of persons who are already subject to legal restrictions against entering school property or determined to pose a possible threat to students, staff and the school community through the school's existing threat assessment procedures. Robust policies and procedures guiding staff engagement following a notification are critical to the success of such applications.



PASS
Partner Alliance
for Safer Schools

passk12.org



PASS[®]
Partner Alliance
for Safer Schools

SCHOOL SAFETY AND SECURITY CHECKLIST

TIER 1	TIER 2	TIER 3	TIER 4
--------	--------	--------	--------



DISTRICT-WIDE LAYER

STATUS

YEAR

NOTES

	TIER 1	TIER 2	TIER 3	TIER 4	STATUS	YEAR	NOTES
• POLICIES AND PROCEDURES							
» Dedicated Security Director/Department	✓	✓	✓	✓			
» Establishment of Safety Policies and Procedures	✓	✓	✓	✓			
» District-Wide Physical Security Standards	✓	✓	✓	✓			
» Annual Physical Security Assessments Based on District-Wide Standards	✓	✓	✓	✓			
» Ensure Maintenance of Security Technology Implementations	✓	✓	✓	✓			
» Pre-Approval of Applications for School-Issued Electronic Devices	✓	✓	✓	✓			
» Conduct Lockdown Drills	✓	✓	✓	✓			
» Independent Security Assessment on 3-Year Cycle				✓			
VISITOR MANAGEMENT SYSTEM							
» Visitor Badging System	✓	✓	✓	✓			
» Electronic Visitor Management System		✓	✓	✓			
» VMS-Assisted Background Checks				✓			
STUDENT AND STAFF IDENTIFICATION							
» Volunteer Background Checks	✓	✓	✓	✓			
» Smart Card Identification Badges			✓	✓			
• ARCHITECTURAL							
» Facility and Vicinity Mapping	✓	✓	✓	✓			
» Entrances Marked With First Responder Numbering System	✓	✓	✓	✓			
» Printed or Electronic "Tactical Floor Plans"		✓	✓	✓			
» Zone Emergency Response System			✓	✓			
» Virtual Response Plans and Implementation				✓			
• COMMUNICATION							
» Wide-Area Two-Way Radio System	✓	✓	✓	✓			
» Bi-Directional Amplifier (BDA) or Distributed Antenna Systems	✓	✓	✓	✓			
» 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			✓	✓			

TIER 1	TIER 2	TIER 3	TIER 4
--------	--------	--------	--------



DISTRICT-WIDE LAYER (cont.)

STATUS

YEAR

NOTES

• ACCESS CONTROL

» Emergency Site Building Access System for First Responders	✓	✓	✓	✓			
» Access Control System Equipped with Remote Door Release and Lockdown Capability			✓	✓			
» Electronic Access Control for IDF & MDF Rooms w/Key Override				✓			

TRANSPORTATION

» Interoperable Radio System for All Buses and School Vehicles	✓	✓	✓	✓			
» Bus Video Surveillance/GPS System		✓	✓	✓			
» Bus Video Surveillance System		✓	✓	✓			
» Card-Based Check-In				✓			

• VIDEO SURVEILLANCE

» Incorporation of Video Surveillance Into Emergency Response Plans	✓	✓	✓	✓			
» Camera Standardization		✓	✓	✓			
» Recording System Standardization			✓	✓			
» Video Verification of Intrusion Alarms to Monitoring Service, Administrators and/or SOC				✓			
» Video Verification of Duress Alarms to a Monitoring Service, Administrators and/or SOC				✓			

• DETECTION AND ALARMS

» Centrally Monitored Intrusion and Duress Alarms	✓	✓	✓	✓			
» Duress Alarms Sent to Law Enforcement		✓	✓	✓			
» Graphical User Interface for Operators			✓	✓			
» Intrusion and Duress Alarms Monitored by a District-Wide SOC				✓			

TIER 1	TIER 2	TIER 3	TIER 4
--------	--------	--------	--------



PROPERTY PERIMETER LAYER

STATUS

YEAR

NOTES

• POLICIES AND PROCEDURES

» Implement NCS4 Best Practices for Outdoor Activities and Events	✓	✓	✓	✓
» Annual Assessment of Safety of Ground (including Lighting)	✓	✓	✓	✓
» Create Grounds and Facility Use Policies for Outside and Public Groups	✓	✓	✓	✓
» 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			✓	✓
» Install Audio/Video Call Boxes at Key Locations				✓
» 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	✓	✓	✓	✓
» Infrared (IR) Cameras or Lighting		✓	✓	✓
» Wireless Video Data Transmission		✓	✓	✓
» PTZ Camera Coverage		✓	✓	✓
» Perimeter Video Analytics				✓

TIER 1	TIER 2	TIER 3	TIER 4
--------	--------	--------	--------



PARKING LOT PERIMETER LAYER

STATUS

YEAR

NOTES

• POLICIES AND PROCEDURES

» Parking Tags	✓	✓	✓	✓			
» Assign Staff to Periodically Check Parking Lot		✓	✓	✓			
» Persistent Staff Patrol			✓	✓			
» RFID Parking Tags			✓	✓			
» Staff Capability to Initiate Emergency Protocols From Exterior				✓			

• ARCHITECTURAL

» Signage (Directing to Appropriate Areas)	✓	✓	✓	✓			
» Signage Directing to Emergency Communication Device	✓	✓	✓	✓			

• COMMUNICATION

» Wide Area Mass Notification System (MNS)			✓	✓			
» Two-Way Emergency Phones			✓	✓			
» Install Audio/Video Call Boxes at Key Locations				✓			
» Audible and Visual Mass Notification Tied to District-Wide System				✓			

• VIDEO SURVEILLANCE

» Fixed Camera, Wide Area Coverage	✓	✓	✓	✓			
» People Identification Field of View at Pickup/Drop-off Area		✓	✓	✓			
» PTZ Camera Coverage			✓	✓			

TIER 1	TIER 2	TIER 3	TIER 4
--------	--------	--------	--------



BUILDING PERIMETER LAYER

STATUS

YEAR

NOTES

• POLICIES AND PROCEDURES

» Categorization of All Exterior Openings	✓	✓	✓	✓
» Policy Established for Control of Exterior Openings	✓	✓	✓	✓
» Key Control Procedures	✓	✓	✓	✓
» Complete BDA/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)	✓	✓	✓	✓
» Secured Vestibule	✓	✓	✓	✓
» BDA/DAS System (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	✓	✓	✓	✓
» Cylinder Dogging with Indicator	✓	✓	✓	✓
» Door Status Monitoring (Door Position and Latchbolt Position)	✓	✓	✓	✓
» Electronic Access Control of Primary Entrances	✓	✓	✓	✓

• VIDEO SURVEILLANCE

» Video Intercom at Visitor Entrance Points	✓	✓	✓	✓
» Interior, Fixed Camera Coverage for All Entrance Points	✓	✓	✓	✓
» Exterior, Fixed Camera Coverage at All Entry Points		✓	✓	✓

• DETECTION AND ALARMS

» Intrusion Detection System on all Exterior Access Points	✓	✓	✓	✓
» Intrusion Detection System Monitored 24/7	✓	✓	✓	✓
» Partitioned Intrusion Detection			✓	✓

TIER 1	TIER 2	TIER 3	TIER 4
--------	--------	--------	--------



CLASSROOM/INTERIOR PERIMETER LAYER

STATUS

YEAR

NOTES

• POLICIES AND PROCEDURES

» Classroom Doors Closed and Locked When Occupied	✓	✓	✓	✓			
» Designate Shelter Areas Outside Corridor Line of Sight	✓	✓	✓	✓			

• 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)	✓	✓	✓	✓			
» Local Area Two-Way Radio System for Select Staff	✓	✓	✓	✓			
» Two-way Intercom System With Call Buttons		✓	✓	✓			
» Duress Button System - Office and Classroom		✓	✓	✓			
» Local Area Two-Way Radio System for All Staff, Including Teachers		✓	✓	✓			
» In-Building Emergency Communication System			✓	✓			
» BDA/DAS System			✓	✓			
» 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

» Classroom and Shelter in Place Doors Equipped with Office/Entry, or Classroom Security Function Locks	✓	✓	✓	✓			
» Locks with Visual Indicator		✓	✓	✓			
» Stand-Alone Electronic Locks With Fob			✓	✓			
» Networked Electronic Locks				✓			

TIER 1	TIER 2	TIER 3	TIER 4
--------	--------	--------	--------



CLASSROOM/INTERIOR PERIMETER LAYER (cont.)

STATUS

YEAR

NOTES

• 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		✓	✓	✓			

• 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				✓			



PASS[®]
Partner Alliance
for Safer Schools

passk12.org