Electronic Security Guidelines for Schools

An Aid for Schools Considering Procurement of an Electronic Security System

Electronic Security Association
6333 North State Highway 161, Suite 350
Irving, TX 75038
Toll Free: (888) 447-1689
Phone: (972) 807-6800
Fax: (972) 807-6883
Web site: www.ESAweb.org

Foreword

The Electronic Security Association is proud to provide these Guidelines as a resource for the education community. We recognize that schools are under increasing pressure to do all they can to ensure a safe school environment. It is our hope that these Guidelines will offer important assistance in making decisions about the use of electronic security systems as part of an overall effort to keep our children safe.

These Guidelines represent a consensus of opinion by subject matter experts with experience in securing school campuses. Use of these Guidelines is voluntary. Neither ESA, its members, nor the members of the panel of experts are responsible for the use of these Guidelines.

These Guidelines are available for free public download at www.ESAweb.org/schoolguidelines.

For feedback or questions on this project, contact ESA at schoolsecurity@ESAweb.org.

ABOUT ESA

Established in 1948, the Electronic Security Association (ESA) is the largest trade association representing the electronic life safety and security industry. Member companies install, integrate and monitor intrusion and fire detection, video surveillance and electronic access control systems for commercial, residential, industrial and governmental clients. In cooperation with an alliance of chapter associations, ESA provides technical and management training, government advocacy and delivers information, advice, tools, and services that members use to grow their businesses and prosper. ESA may be reached at (888) 447-1689 or on the Web at www.ESAweb.org.

Table of Contents

1. Introduction

1.1. Purpose

This document is intended to provide useful information to school boards, administrators, and community officials who are interested in electronic security systems as part of their overall school security plan. It is meant to inform and advise decision makers about their options in obtaining electronic security systems. This document also makes recommendations for good practices in security evaluation and needs assessment, and in obtaining professional assistance during the procurement process.

1.2. Application

This document is primarily written for public primary and secondary schools (K-12), but parts of these recommendations might be useful to private schools and similar institutions, such as pre-school, daycare, churches, and nursing homes. Parts might also apply to higher education, although the campuses of colleges and universities generally have a distinctly different set of needs than K-12 institutions.

1.3. General Approach

This document is not prescriptive. It is not a specification, nor a comprehensive set of requirements. This document emphasizes certain important points for consideration, and highlights areas for follow-up with professionals.

Since each school property is unique, electronic security must be customized to each facility. Therefore, no single solution can be recommended for all schools. Instead, this document highlights typical factors to consider, common practices among schools, and recommended outreach in aspects that vary by local factors. Likewise, since absolute protection is not possible, the recommendations made are offered as general guidance to help schools make good tradeoffs in their security decisions.

The primary goal of these recommendations is to help protect students, faculty, staff, and visitors by providing an environment where active threats and potential dangers can be mitigated. Protecting other assets, including property and material, is a secondary goal.

2. Assessment Of Threats

2.1. Overall Security

Electronic security is part of an overall *Security Plan*, based on a *Security Survey* conducted to identify threats and vulnerabilities to threats. A full security self-audit and reassessment should

be conducted annually as part of general due diligence, and the assessment should be kept current with any changes that are made to the school facilities, activities, or policies throughout the school year.

Many schools find that the summer months are an ideal time to install a security system. However, a comprehensive appraisal of security needs is best done during the school year when students and faculty can be observed and consulted.

While security professionals are available to assist in the evaluation, a self-audit prior to engaging a professional is both cost-effective for the school and a prudent regular exercise. It will also enable the school to have a more meaningful dialogue with prospective security contractors and ultimately with their chosen security company.

>>> See Section 10 Additional Resources for suggestions on conducting a security self-audit.

2.2. Building Your Team

The school administrator should designate individuals to fill key functional roles on the internal security team. Titles will vary, and a single person might perform more than one functional role, but these areas of responsibility should be included:

- *Safety Manager (or Risk Manager)*
- *Security Manager*
- *Facilities Manager*
- *IT Manager*

>>> See Section 5.3 Team Member Roles for more information on how the school team interacts with security contractors during the procurement process.

External team members should include first responder liaisons and community stakeholders:

- School Board liaison
- Life Safety liaison
- Law Enforcement liaison

The school administrator should also seek the advice of qualified security professionals early in the planning process. Security consultants can help coordinate among team members and outside agencies.

2.3. Documentation

A facility documentation package should be prepared, consisting of current and accurate drawings, which should include:

- Site plan
- Floor plans
- Fire escape plans
- Layout drawings for existing electronic systems (noting the brands of those systems)

- Sketches of any planned construction
- Any emergency processes and procedures that have been implemented
- A record of who has authorized access to the interior and exterior areas of the school
- A current list of key holders and access control card holders if there is an existing access control system (key and card audit report)
- Emergency call list (for fire and security responders)

When drawings are not readily available, the school can often contact outside sources for drawings of their facility. These might include:

- Original building architects (if possible)
- Local fire department
- City hall for public records

Drawings might be on paper or electronic (in Visio™ or other similar CAD system format).

If facility drawings cannot be found, a basic layout drawing should be created by hand and used for emergency planning and discussion with potential contractors during their site surveys.

Copies of current facility drawings/plans, in paper or electronic form, should be given to local law enforcement and life safety officials to help them better prepare for any situation at the facility that would require their response.

>>> See Section 12 Samples and Checklists for a summary of recommended documentation.

School administrators should consider the use of software products that can significantly ease the burden of records management and preparedness inventories.

2.4. Types Of Threats

Internal and External: The planning team should consider all areas of vulnerability, and identify both external and internal threats. While intrusions are a concern, the behavior of students is often the most likely cause of an emergency situation, involving “active threats” from students who are already in the school or have access to the school.

The planning team should consider who has access to the school and include threats from lost or stolen keys, especially master keys, and assess the need to re-key or replace locks.

Schools should review all activities that take place at the school in terms of potential threats. Electronic systems can be configured to accommodate these activities for both normal use and special situations.

>>> See Section 7 Modes of Operation for more information on how systems can accommodate school activities.

2.5. Layers of Protection

School security is often thought of in layers or rings:

- **Outer Perimeter** – parking lot, adjacent athletic field, outlying buildings
- **Building Perimeter** – with primary and secondary entry points
- **Interior Spaces** – classrooms, staff offices, hallways and stairwells, cafeteria, gymnasium, auditorium

Each of these areas has access by different types of occupants, and they are usually considered as unique partitions of the campus in the security system layout and control. Special technologies and system uses apply to each area of campus. For example: The perimeter doors might be secured with a basic Intrusion Detection system, while select doors might have Access Control, and large interior spaces like the cafeteria might have cameras for Surveillance.

Security professionals can advise on all aspects of threat assessment, conduct a security survey, and recommend appropriate solutions for each unique facility.

3. Scale and Funding Considerations

3.1. Decision Maker Approvals

The school should hold community consultations early, giving all affected parties an opportunity to provide input and to prepare for coming potential changes.

These parties include:

- school board
- parents
- faculty
- staff
- students (a frequently underestimated input)

Holding early consultations with stakeholders and keeping them informed throughout the planning process will greatly facilitate both formal budgetary approvals and acceptance of the security measures that are eventually undertaken.

3.2. Compatibility with Existing Equipment

Non-proprietary (off-the-shelf) or Proprietary: Non-proprietary equipment is generally more cost effective in the long run, more likely to ensure compatibility with other equipment (existing and future), and allows more flexibility in choosing contractors for support or upgrades. Proprietary equipment is usually available from and serviced by a sole vendor. Proprietary equipment might be needed to extend an existing proprietary system instead of replacing it, or for special advanced applications.

Software products should use open architecture and IP-based communications to allow compatibility across product lines and ease the addition of new applications in the future.

Video systems should use commonly accepted and current video formats for transmission, display, and recording.

3.3. Future Planning

Scaling: The school should consider future growth and backward compatibility. Some systems can be implemented with phased-in additions for multi-year budgeting. (For example: Extra cabling can be run during the installation, but only some of the card readers or cameras installed in the first year.)

Infrastructure: The school should consider other planned construction and purchases. It is usually more cost-effective to include the security system infrastructure (or *rough-in* stage) in planned construction, especially construction involving pavement. Also, some systems are used for multiple purposes, and the costs for updates and growth can be shared across projects. (For example, if the school is already planning to update their telephone system or computer network, the security system can take advantage of the upgrade without adding redundant costs.)

Recurring costs: Budgetary planning should include annual fees for licensing and permits (including routine inspections), lost and new cards or tokens, ongoing maintenance, remote monitoring services, signage, data backups, and data/video storage.

>>> See Section 8 System Integration and Installation for additional information on the stages of system installation.

3.4. Funding Sources

School administrators should contact local authorities to collaborate on ways to seek and obtain funding. They should also consider the additional and extended uses of the security systems, when assessing the return on investment, such as using cameras to improve teaching effectiveness.

Some of the possible funding sources include:

- **User Fees** – cost offsets, one-time initial fees, recovery of recurring costs (such as for lost access cards)
- **Sponsors** – private donors, alumni associations
- **Public-Private Partnerships** – agencies that work with private industry in community safety programs
- **Bond Elections** – local government funding, voted on by the local community
- **Government Grants** – federal funds for emergency preparedness, direct or matched to local government funding

>>> See Section 10 Additional Resources for more information on available grants and how to apply for them.

Security professionals can also provide valuable advice on budgetary tradeoffs, cost recovery, and options for installing a system in phases.

4. Cultural Considerations

4.1. Safety and Convenience Tradeoffs

School administrators often find that the culture and behavioral practices of the faculty, staff and students are obstacles to increasing the physical security of their facilities. All affected parties should be encouraged to overcome the common desire to keep doing what they are used to and appreciate that the changes in their routines are made for safety.

The school administrator should help all school personnel understand how they will use the system and what to expect. This should include good communications throughout the planning stages to manage expectations and training on how to operate the system once it is installed.

All parties should be made aware that the security system will cause changes to traffic patterns and allowed freedom of movement for students, staff, and visitors. The security system will limit ease of access through secondary entry points.

A desired level of convenience for entry and exit can sometimes be accomplished by adding components, but with a tradeoff in added cost, such as card readers on more doors instead of alarms to provide more controlled entry points on secondary doors.

The school team should also balance safety and privacy. Disclosure of video or audio monitoring through signage might be required by local laws.

Through good design, schools can provide an atmosphere that feels warm and inviting, yet secure.

4.2. Activities and Visitors

The school team should review typical activities and routines, both during school hours and after-hours, as well as the typical types of visitors they expect. The team should also review desired alternate uses for the school, special events, and multi-purpose areas.

The school's activity profile is very important in the security system design. Some modes of system operation can be programmed and are more easily revised after installation (such as the length of time a door stays open before a warning is detected), but other modes are built in and should be decided early (especially areas that affect the cabling infrastructure). The school team should discuss flexibility of reconfiguring the system with potential security contractors.

>>> See Section 7 Modes of Operation for more information on how systems can accommodate school activities.

4.3. Community Values, Demographics, and Crime

Many local factors affect the school's choice in system operation and performance. These include community expectations for the atmosphere at the school and the types of crime in the surrounding area. Local law enforcement can often provide useful crime data and historical analysis that will influence the desired security system, such as types of crime and times of year that are prone to higher crime rates. The school team should be prepared to discuss these less tangible factors with security professionals during their security surveys.

4.4. Local Laws and Codes

Local laws and building codes significantly affect the system design and layers of protection. Schools should consult their local police department and fire marshal for advice on laws regarding the rights of the public to school access, items that may not be brought into schools, requirements for construction methods, and required inspections.

5. Selection of Contractors

5.1. Types of Procurements

Not all schools will follow a formal procurement process with multiple bidders, but each will face similar decisions in choosing a contractor. Because each electronic security system is customized to the unique conditions of each school, the proposal stage takes a significant investment of time and effort, from both the school security team and potential contractors.

The following are the typical types of procurements:

- **Develop a Specification for Bid and select from multiple Integrator proposals**: This method relies on a *Consultant* for the initial security evaluation and a separate *Integrator* for system design and installation. The Integrator is selected from among the proposals of several candidate Integrators. The proposals also contain terms of installation and warranty. The Consultant prepares the performance Specification and often helps in evaluating the design proposals as well. The Consultant should remain available after selecting an Integrator for a smooth transfer of information and to answer questions that arise during installation. Depending on the size of the school district's procurement team, some consultants can assist in preparation of the bid request, vendor review, and project management.
- **Evaluation and Design from one Integrator**: This method is less formal and is often adequate for smaller facilities and single schools. A school might still ask for proposals from multiple integrators, but no Specification for Bid is developed first. The proposals in this case will include a security evaluation along with a system design and the terms of installation and warranty.

- **Designated Designer/Integrator**: A preferred Integrator might be designated when efficiencies can be gained by combining related work, for expansion or updates to an existing system previously installed by the Integrator, or for multi-year projects.

Decisions on which method to use depend on available school resources, and sometimes local requirements for competitive bids in public procurements. Engaging a separate Consultant for evaluation and Integrator for system design is common for large scale installations; it has additional costs, but it generally increases the objectivity of the design.

5.2. Solicitations

Solicitations are used to gather information from potential providers and are generally of these types:

- ***Request for Information*** (RFI) – to determine who is interested and their capabilities
- ***Request for Quote*** (RFQ) – to obtain a simple price quote, usually for early or general budgetary planning
- ***Request for Proposal*** (RFP) – to obtain a proposal with a system design, price quote, and terms of fulfillment

Sample solicitations can be obtained from public records and other schools, but care should always be taken to adjust any examples to each school's unique needs.

5.3. Team Member Roles

During the procurement, a *Security Survey* is conducted by the security consultant (if one is used) and separate site surveys by each of the candidate security contractors (if no consultant is used). Various members of the school team should be available to work with these security professionals during the surveys, during proposal evaluations, and again during system integration and installation by the chosen Integrator.

The school team should review their threat assessments and cultural considerations from earlier internal planning and self-audit, both during the initial security consultation and the security surveys by Integrators.

The following are functional roles that will be needed, although one person might be responsible for more than one function:

- ***Consultant*** (provider role) – an individual who provides professional or expert advice in the design and implementation of a security plan. The Consultant will conduct a security survey, interview members of the school staff and security team to gather information on their specialty areas, and coordinate with outside liaisons to gather information about local requirements. A Consultant can provide advice on overall security needs, help develop a specification for an electronic security system, and help evaluate design proposals. The Consultant should never accept any form of remuneration based on

equipment or suppliers recommended during the project, nor engage in any activities that would present a conflict of interest that could compromise objectivity.

- ***Integrator*** (provider role) – an individual or company capable of installing and programming a variety of systems, such as a Security Alarm, CCTV, Access Control, Fire Alarm, Lighting, Gate Operations, and Locking Hardware, Intercom Systems; and enabling these systems to work together to create a complete security and life safety solution for the end user. An Integrator conducts a security survey, proposes a system design, installs the security system, and provides service under warranty and separate maintenance contracts. The Integrator coordinates with the school security team, local authorities, and other affected parties. An Integrator might use subcontractors for highly specialized parts of the security system.
- ***Safety Manager*** (customer role) – the individual responsible for ensuring that systems, procedures and applications do not create an unsafe situation or condition. The Safety Manger will help revise standard operating procedures to include the new security system.
- ***Security Manager*** (customer role) – the individual responsible for administrating the security system operation, use, and maintenance. These responsibilities include issuing credential media, setting levels of access, determining time/day restrictions of system users, and maintaining the key and card audit report. The Security Manager also oversees video monitoring operations and interfaces with any security service providers used, such as private guard services and remote monitoring stations for alarm systems.
- ***Facilities Manager*** (customer role) – the individual responsible for building physical and structural maintenance, utility management, construction, custodial services, etc. The facility manager generally maintains the building drawing package and might assist in periodic inspection and preventative maintenance of the security system.
- ***IT Manager*** (customer role) – the individual responsible for the school's computer networks and equipment. The IT Manager works with the Integrator to ensure that the security system design is compatible with the school's other data and telecommunications networks. The IT manager might also be responsible for data backups, video storage, password management, and network security.

5.4. How to Find and Screen Potential Contractors

School administrators should seek referral sources from other schools of similar size and demographics.

School administrators should contact their state chapter of ESA for listings of local Integrators, and ask potential contractors if they are members of ESA.

School administrators should ask Integrators for evidence that they have the following credentials:

- **Company** – meets state and local requirements for licensing and insurance; follows ESA Code of Ethics and Standards of Conduct

- **Installers and Technicians** – have nationally recognized training such as National Training School (NTS) including continuing education; have vendor-authorized training on the products used; have special training if video cabling is used, and all have undergone a background check
- **Special Certifications** – might be required in some states and for certain specialized systems (such as for fire systems or eligibility for grants)

Qualifications should be determined by factors such as:

- **relevant experience** with enterprise level facilities of similar scope and size
- **ability to service** the system after installation, proximity of their service center and typical response time to service calls

Proposals should be evaluated through a qualitative evaluation for best value, not necessarily the lowest bidder. Overall, the school should seek to find the right security partners early and keep them involved throughout.

When requesting proposals from Integrators, school administrators should ask for detailed information on the products proposed, the rationale for their selection, and available configuration options. Proposal evaluators should review the selection rationale and expected performance of the devices in the proposed systems.

Additional information on products and their intended uses is available online from product manufacturers and can be helpful when reviewing proposals.

6. System Equipment Options

This section provides a general description of the security equipment used in school settings to encourage basic familiarity with the terms used and facilitate a better discussion between the school team and security professionals. School administrators should discuss these options with their security team and make decisions about the exact configuration and features that are best suited to their needs.

Most security systems include more than one sub-system type. Most are integrated with other low-voltage systems, existing and new, such as the intercom system, the phone system, and the fire detection/notification and suppression systems (fire alarm and sprinklers). Special consideration is always given to integration with the fire alarm system and always allows egress.

All electronic systems use some type of wiring infrastructure. Some systems use very specialized cabling, such as those using video. Some systems have the ability to utilize wireless technology to broadcast data and video.

In general, all systems should meet state and local requirements, such as building codes, and many require inspection by an *Authority Having Jurisdiction* (AHJ).

6.1. Access Control

An Access Control system is made up of doors, frames, hinges, door closers, gates, locks, keys, card readers, cards and tokens, biometric readers, and software.

Entry/exit points fall into these general categories:

- Primary (main entrance)
- Secondary (exterior doors)
- Other (interior openings, grouped into partitions of the building)

Doors are viewed in terms of their use and location, which affect both their construction and how they are to be secured.

Some doors are required by local laws to meet certain fire safety codes, such as providing a fire separation barrier, and the requirements extend to compatible door hardware and locking mechanisms to ensure they do not compromise life safety. School administrators should seek advice from the local Authority Having Jurisdiction (AHJ) early in the procurement regarding construction requirements for life safety, particularly in the selection of locks.

Some doors can be an integral part of shelters designed for hurricane or tornado. Some door closure patterns can affect air circulation and indoor air quality through air leakage from the building envelope.

Building occupants (staff, students, and visitors) should be given different access rights to the school or certain parts of the school. (For example: Faculty access 24/7. Coaches access athletic facility 24/7. Students access during school hours. Parents access during school hours, when authorized by main office.)

Visitor access should be directed to a single primary entry point by keeping secondary entry points locked and using signage to direct external traffic to the main entry point.

Controlled access through a primary entrance is commonly used to provide a *secure vestibule* or *sally port*. The outer door is typically unlocked during normal school hours; the interior set of doors are locked during school hours, but allow free egress. Interior doors are controlled by a card reader (for faculty and staff), or they can be controlled from the main office (for visitors). They can be unlocked remotely for a momentary period of time, and then return to a secured state. The main office can provide access by using a button to release the electronic lock or by using an access control software interface. Visitor verification can be done by viewing with a camera or communicating through an intercom.

Temporary badging offers added control for visitors, as well as temporary staff (substitute teachers or temporary custodians) and contractors. These system users should be given limited access by location or time of day, and their badges should be automatically disabled when no longer needed.

6.2. Surveillance

A Surveillance system is made up of: cameras, special cabling, and a Monitoring system. It can also be integrated with an Intrusion system and Access Control system.

Cameras are often placed at exterior doors to verify alarms or screen visitors. They are also used for large areas (interior and exterior) to monitor certain activities or provide safe passage along certain routes of transit for students and staff.

Camera capabilities include a large variety of options, but they should support IP-video transmission, and they should be selected based on the manufacturer's specifications for their intended use. The environmental conditions around the intended camera locations should also be considered. (For example: A wide angle view would be appropriate for large areas, but not for looking down a narrow hallway.) The intended use of the camera includes use of the captured video, since a higher resolution might be desired for forensic analysis than for active monitoring with real-time response or for simple visitor verification.

School personnel should be realistic about preconceived expectations. While camera technology is advancing rapidly, there are generally tradeoffs between capabilities and costs. Crime shows on TV often use advanced technologies that are not currently in the affordable mainstream.

6.3. Monitoring and Supervision

A Monitoring system is made up of display screens, video and data (for status of system), and video recording devices.

Active Monitoring (or *Response Monitoring*) is performed by personnel watching live feeds on a display screen, usually with the intent of providing immediate response to an event.

Passive Monitoring (or *Forensics Monitoring*) is recorded and viewed or analyzed at a later time, usually as part of an event investigation.

Various kinds of video analytics can be used for either type of monitoring (Response or Forensic), to detect patterns in the video. Analytics can be done remotely or in a separate system if common compatible data formats are used.

Monitoring for schools is usually done on site, but it can be done remotely by professional monitoring service providers as a full-time or part-time supplemental service. In either case, the school should decide as a matter of policy who can view the video.

Some monitoring systems can be configured to send live feed to responders during an incident. This can be very advantageous for crisis management, but it should be coordinated closely with local public safety during the system design.

Integrators can provide advice on the selection of monitoring points, including recommended views under various conditions and at different times of day, and recommend appropriate video resolution for the application. (Resolution can be different for video display and video recording.)

Recording can be continuous, alarm activated, or a combination of the two.

The school's video retention policy should consider the number of days of recording to keep, the quality (higher resolution takes a higher capacity storage media), and whether all video should be kept or just video from alarm events. Provisions should be made for adequate storage capacity, bearing in mind that HD video requires larger storage capacity.

Supervised perimeter alarms are monitored through software as part of an Intrusion system. The alarm state signal generated in an Intrusion system shows up on a display that indicates the system status and which part of the system was activated by an event. The alarm signals can be monitored on-site or at a remote monitoring station. Many public safety jurisdictions have requirements that the alarms be verified by a secondary means before responders are called.

6.4. Intrusion

Intrusion detection systems (burglar alarms) are used for perimeter control, for either an outer perimeter or the building perimeter. These systems are not usually used during school hours.

Intrusion systems are sensor driven and activate alarm warnings when a violation of the perimeter is detected, such as open doors, motion detected, broken glass, etc. The alarm status activates the Communication system, sounding local alarm annunciators (bells and sirens) and calling a monitoring station for verification, possibly by on-site guards or captured video. Intrusion alarms can automatically activate video recording.

6.5. Personal Panic Buttons

Panic buttons are usually part of a more general Intrusion system. The buttons can be placed in fixed locations for key staff, such as main office reception personnel, or portable devices can be used by certain school staff, such as those who work late hours or work with high-risk students. Some portable devices include location capability.

The alarm signals sent by these devices should go to a monitoring center (internal or external) with a means of verifying the alarm, not direct dial to first responders.

6.6. Communication

The Communication System includes parts of several other systems, wired and wireless, such as:

- **Intercom Systems** (video and voice, used for entry verification or for general school communications)
- **Local Alarm Annunciators** (for fire, intrusion, and other emergencies)
- **Internal Notifications** to classrooms through smart boards or staff cell phones
- **External Calls** to 911, police, private responders, or fire department (includes voice and text, includes automated and manual initiation)
- **Two-Way Radios** used by staff or guards (not considered part of the electronic security system, but can be used to compliment the system during emergencies)

All parties in the school should understand the sequence of automatic system responses to all anticipated events and make those part of their overall emergency response protocols.

6.7. Mechanical Devices and Materials

Locks and Keys: In most cases a blended solution including both electronic locks controlled by an access control software system and mechanical locks will be used to secure a school. Both electrified and mechanical locks should be Grade 1 Commercial and appropriate to the type of door (per the manufacturer's specifications). School administrators should ask for detailed information on the locks proposed by Integrators, including specifications from the lock supplier.

The Security Manager should locate and track all keys. This is a critical area of vulnerability and often overlooked. Key tracking software can be used to create a database or spreadsheet of who was issued which keys, in addition to many other details regarding key control. Electronic key control boxes are commonly used to issue specific keys or rings of keys to custodial and maintenance staff, which are returned daily.

Areas around doors often present vulnerability, especially glass panels. Some materials and products can offer cost-effective security upgrades, such as security screens or laminated safety film instead of bullet-proof glass. In general, the school administrator should keep in mind that non-electronic products can often be used to supplement security.

The Security Manager should do periodic system reviews that include locks and physical barriers to entry, at least quarterly.

6.8. Lighting and Special Detectors

Lighting is not part of the electronic security system, but should be considered for overall security, especially to provide well lit areas for safe passage. New advances in LED lighting can offer cost savings and dual use for safety lighting. Some lights can be used for communications, such as for emergency exit routes and alert conditions.

Special detectors, such as gas detectors, metal detectors, and substance detectors can be integrated with the main systems discussed above.

6.9. Signage

The importance of the Signage system should not be underestimated.

Signage is used to:

- **Direct visitors** toward desired main entry point
- **Deter undesired activities**, such as "no trespassing", "drug-free zone", "this area monitored by cameras", etc. (Signage has tremendous deterrent value. Schools should seek advice from local authorities for recommended signage.)
- **Inform visitors** of surveillance, especially video and audio recording (Disclosure might be required by local laws.)
- **Direct occupants in emergencies** toward designated safe areas or evacuation routes

7. Modes Of Operation

Security systems can be configured for several pre-determined modes of operation based on the various uses of the school at different times and the expected activities of the occupants. Systems are generally divided into partitions that can be controlled separately.

The school team should discuss the desired operation of the systems with the integrator or consultant during design, taking care to explain the various patterns of activity in the school.

7.1. Normal, Special, and Emergency

Normal operation accommodates routine traffic patterns during normal school hours in the various areas (or partitions) of the campus.

During school hours, the primary focus should be on controlling access to interior and exterior openings, monitoring activities, and communicating with occupants. Systems such as Access Control, Surveillance, and Communications are used. Intrusion detection systems (burglar alarm systems) are not intended to be active when schools are occupied.

Special operation includes after-hours activities, special events, or special visitors.

The various partitions of the Access Control system can be changed to allow visitors more access to certain areas for special events. Surveillance and Monitoring needs will change during special events.

Special visitors can be given different levels of access to all or some areas of campus. The Intrusion system is used at night when the building is not occupied.

Emergency operations occur when there is an active threat, which can range from a student altercation to an active shooter, a fire alarm from a detector or a pull-station, a natural disaster, or a power loss.

In this mode of operation, the system can help direct students to shelter in place, to be on guard but await further instructions, or to evacuate.

7.2. Lockdown and Egress

Policies for building lockdown, both when and how to do it, vary across the country. School administrators should check with local authorities for their desired policy and ask security professionals to recommend ways to accommodate the policy with new technologies.

Lockdown can be controlled locally (each door individually) or from a central control, locking all internal doors and external entry points simultaneously.

First responder access can be provided with special access cards, given to select first responders in advance of an incident, which will allow them to enter a building in lockdown through the access control system. Most AHJs require a “Knox Box” or similar exterior mounted key box that only responding fire or police personnel can open to access the needed building keys.

Locking systems should be configured to always allow egress. Codes for fire and life safety require it. The security system should never compromise the fire detection and fire suppression systems, nor impede normal occupant egress. Electronic locks should provide power loss defaults or manual overrides that allow for occupant escape. School administrators should consult with their local AHJ’s on all matters regarding locks and egress.

Security professionals should be well versed in local building codes and prevailing laws. They can coordinate with the necessary parties and advise the school administrator of requirements and options for modes of system operation.

8. System Integration and Installation

During Integration and Installation, the school security team will work with the chosen security Integrator to arrange access for installers and technicians, and discuss any questions that arise.

8.1. Involve Key Stakeholders

The school team should review the threat assessment and cultural considerations, and adjust the design if necessary. All stakeholders should be kept informed of the decisions and tradeoffs being made during this process. All affected parties should be notified of the work being done, including the community, faculty, students, parents, other frequent visitors.

8.2. Stages of Installation

Rough-in: This is when the infrastructure is installed, including conduit and cabling.

Finish: This stage involves mounting components, such as cameras and card readers, connecting them to the infrastructure wiring, and then programming the system software.

Commissioning: The final stage of deployment is the system test and customer acceptance.

School administrators should anticipate inspection to codes by an AHJ.

During system test, the security team should request a full run-through of all system functions, both in normal and emergency states. The test should include all other systems affected, even existing systems that were modified.

8.3. Documentation

Upon completion of the installation, the Integrator should provide “as-built” drawings showing device locations, interconnectivity, and wiring. In addition, the Integrator should provide the operation and maintenance manuals for each piece of equipment installed.

As the security system installation is completed, the school should review and revise all standing security plans, such as Standard Operating Procedures, emergency drills, and inventories of keys and access cards.

The school should develop an overall Security Awareness Program that incorporates use of the new security system into student and staff safety vigilance.

>>> See Section 13 Additional Details on Select Topics for more information on creating a Security Awareness Program.

9. System Use and Maintenance

9.1. Responsible Parties

Responsible parties should be determined by the type of system and its routine functions. In an Access Control system, these will include someone to issue access cards, change access privileges, and monitor inventories of cards and keys. A different person might be responsible for screening and letting in visitors, or for initiating a centrally controlled lockdown. For Surveillance, responsible parties will include someone to monitor the video and manage backups.

Each person should be clearly designated with clearly identified responsibilities.

9.2. User Training

Operators who are charged with controlling the system or monitoring its status should be provided with system training by the Integrator. All system users, including staff and students, should be given an orientation on the new security system, including routine operation and what to expect in an emergency. This orientation can be conducted by members of the school security team based on recommendations and supporting materials provided by the Integrator.

The security team should include police or private security responders in practice sessions with the new system. This should be used as an opportunity to build relations with local public safety.

9.3. Maintenance

The school Security Manager should conduct periodic visual inspections of both the electronic and mechanical components, at least quarterly, and provide routine preventative maintenance for environmental degradation.

The Security Manager should perform periodic functional tests, especially if alterations or repairs have been made to inter-connected systems.

A point of contact for the service provider and an expected response time to service calls should be established prior to accepting the system.

9.4. Documentation

The Security Program documentation package should be kept current, revising the drawings as appropriate whenever alterations are made to the security system or to inter-connected systems**.**

The Security Manager should maintain an ongoing relationship with the security Integrator after installation, periodically reviewing service logs and operating patterns for potential desired changes to the system operation or programming.

10. Additional Resources for Assistance

These resources offer relevant advice to school administrators on various aspects of project planning, team building, documentation, and funding sources. Many offer references to further resources in specific areas related to school safety and violence prevention.

10.1. Professional Associations

Electronic Security Association (ESA) – find your state chapter, assistance in evaluating Integrator best practices
http://www.esaweb.org/

ASIS International – assistance in finding a security consultant
https://www.asisonline.org/

The International Association of Professional Security Consultants (IAPSC) – assistance in finding a security consultant
http://iapsc.org/

American Association of School Administrators (AASA)
http://www.aasa.org/

National Association of Elementary School Principals (NAESP)
http://www.naesp.org/

National Association of Secondary School Principals (NASSP)
http://www.principals.org/

Association of School Business Officials International (ASBO)
http://www.asbointl.org

10.2. Local Authorities

Local police department – ask for crime reduction division, school resource officer

International Association of Chiefs of Police (IACP) – school safety information and training
http://www.theiacp.org/

National Association of State Fire Marshals (NASFM) – find your State Fire Marshal's office
http://www.firemarshals.org/

10.3. Government Agencies

Homeland Security - assistance with funding
http://www.dhs.gov/school-safety

Homeland Security - assistance with emergency preparedness
http://www.firstresponder.gov/

Federal Emergency Management Agency (FEMA) - assistance with funding
http://www.fema.gov/

10.4. Other Resources

Partnership for Safe Schools – online training on safety preparedness in schools
http://www.theiacp.org/portals/0/pdfs/PartnershipsForSafeSchoolsCourseDescription.pdf

Guide for Preventing and Responding to School Violence
http://www.theiacp.org/LinkClick.aspx?fileticket=MwvD03yXrnE%3d&tabid=378

Digital Imaging for Safe Schools Resource Guide
http://www.theiacp.org/LinkClick.aspx?fileticket=rQSQ9%2b0gB5U%3d&tabid=378

National Crime Prevention Council - Crime Prevention Through Environmental Design
http://www.ncpc.org/topics/home-and-neighborhood-safety/strategies/strategy-cpted-ordinances-guidelines

Homeland Security - BIPS 07: Primer to Design Safe School Projects in Case of Terrorist Attacks and School Shootings, 2nd Edition
http://www.dhs.gov/bips-07-primer-design-safe-school-projects-case-terrorist-attacks-and-school-shootings-2nd-edition

U.S. Department of Education – information on emergency planning, including self-audits
http://www2.ed.gov/admins/lead/safety/emergencyplan/index.html

11. Glossary

This section explains how terms are used in this document, with additional information on the context of the terms in some cases.

There are numerous industry glossaries available from the resources listed above and others, some being very comprehensive and others tailored to a specific kind of system or equipment type.

Active monitoring – live video displayed on a screen and watched by a person
Analytics – software used to evaluate data or video to determine patterns
Authority Having Jurisdiction (AHJ) – a local official with authority to determine compliance to requirements, usually a fire marshal
Consultant – an individual who provides professional or expert advice in the design and implementation of a security plan
Contractor – a company (usually an Integrator) that is hired to provide a security system and associated services, in some cases through the use of specialty subcontractors
Facilities Manager – an individual responsible for building structural maintenance, utility management, construction, custodial services, etc.
Integrator – an individual or company capable of installing and programming a variety of electronic security systems and enabling those systems to work together to create a complete security and life safety solution
IT Manager – an individual responsible for a school's computer networks and equipment
Passive monitoring – recorded video for later viewing, usually to investigate an event
Primary entry point – main entrance to the school building
Request for Information (RFI) – a type of solicitation used to determine who is interested and their capabilities
Request for Proposal (RFP) – a type of solicitation used to obtain a proposal with a system design, price quote, and terms of fulfillment
Request for Quote (RFQ) -– a type of solicitation used to obtain a simple price quote, usually used for initial budget planning
Rough-in – installation of basic infrastructure for a security system, usually wiring and conduit
Safety Manager (or Risk Manager) – an individual responsible for ensuring that systems, procedures, and applications do not create an unsafe situation or condition
Sally port – this term is sometimes used by law enforcement, see *secure vestibule*
Secondary entry point – exterior entry point to the school building other than the main entrance
Secure vestibule – a space between an outer entry point (door or fence) and an inner door
Security Manager – an individual responsible for administrating the security system operation, use, and maintenance
Security Plan – a comprehensive set of security measures to mitigate against vulnerabilities and threats, including emergency response protocols
Security Survey – a comprehensive review of the facility features and school activities, conducted to determine vulnerabilities and threats

Specification for Bid (or Performance Specification) – description of the security system functionality and specific design requirements

12. Samples and Checklists

12.1. Recommended Documentation

✓	Site Plan
✓	Floor Plans
✓	Fire Escape Plan
✓	Layout Drawings for any existing electronic systems (with brands)
✓	Sketches of any planned construction
✓	Emergency Protocols, Standard Operating Procedures
✓	A record of who has authorized access to interior and exterior areas of the school
✓	Key and Card Audit Report: a list of key holders and access control card holders
✓	Emergency call list (for fire and security responders)

13. Additional Details on Select Topics

This section provides more detailed supplemental information for certain security programs, types of equipment, and related subjects, as offered by the participating industry experts.

In addition to the details provided below, the following product areas have been identified for further detailed consideration by schools:

- Locking devices
- Cameras and Video
- Wireless technologies

13.1. Security Awareness Program (SAP)

This section was provided by Ron Lander, a member of the Panel of Security Industry Experts.

A **Security Awareness Program** will positively impact and lessen security threats to both people as well as assets, including the personal property of staff, students and visitors. **SAPs** are analogous to the well-established **Neighborhood Watch Program**. In a sense, the **SAP** moves the **Neighborhood Watch Program** into the school. An important element in cultivating and maintaining the **SAP** will also require leadership by example from all security officers. To quote **Ken Blanchard** of *One-Minute Manager* fame, the idea is to "*catch me doing something right*." This program will draw attention to the positive contributions of employees. However, it will also

spell out what the expected behaviors are as well as the consequences for violating these standards. This program can be promoted through articles in the school's periodic newsletter/website.

All too often the school security program is viewed as someone else's responsibility, or more frequently it is an abstraction without functionality. Security Awareness Programs, not only engage the participation of the faculty and staff, but they even enlist the participation of students to some degree. **SAPs** do come into existence by way of declaration. These programs evolve through an educational process. SAPs must teach the participants how to identify and recognize potential security threats in the incipient stage, and those same participants must be informed as to what actions are appropriate and when to back-off and notify the appropriate authorities.

Another vehicle to help promulgate a **SAP** would be establishing a **Security Awareness Intranet Website**. That site could promote and reinforce the value that security is everyone's responsibility.

The introduction of a **SAP** should start with the training of all employees in how to be more observant of their surroundings. All employees should be trained in how to recognize *suspicious behavior.* This training includes recognition of the clues provided by *body language and speech patterns.* They should also be trained in how and when to interact with suspicious persons. They need to be taught what to say, what not to say, and how to say it.

This ability to recognize and deal with persons who have no apparent legitimate reason to be in the **school** must become a routine portion of the **New Employee Orientation Program** along with the **SAP**. Once the **SAP** is firmly in place, it needs to be continuously reinforced though internal campus' communication media and periodic continuing education initiatives. The establishment and maintenance of a **SAP** intranet site should be considered.

One of the emphases of a **SAP** is to train the users on the tricks and tactics of persons who wish to defeat an access control system, like "coat-tailing", "tailgating" or "social engineering." Participants need to acquire skill-sets such as "How to recognize suspicious persons or groups." Like any security, SAPs are an anticipatory exercise.

Another aspect of the **SAP** is the power of the poster, coaster, calendar and handout. There are several organizations that make large posters and other media available for campuses. The target is mostly IT security, but physical security can also be an integral component. Handouts or brochures can also be distributed during training sessions, staff briefings and the supervisors can have a short script to reinforce the message of the respective promotional piece.

The benefits of Security Awareness Programs are numerous.

- They are low in cost to initiate and to maintain.
- They amplify and add value to existing security programs.
- They amplify the impact of security systems.
- They are a force multiplier for security personnel and school police.
- They build the bridge between the electronic components and the humans who are responsible for managing and using the systems.

Contributors: Panel of Security Industry Experts

ESA gratefully acknowledges the contributions of the following industry experts. The Panel of Subject Matter Experts was balanced to provide representation across type of company (manufacturing, threat assessment, design, and installation), size of company (small businesses and national companies), equipment specialties (subsystems, hardware, and software), and 3 US geographic regions. The Panel consisted primarily of system designers with relevant experience in securing schools (typically 10-15 schools each), and most have extensive experience (10-40 years each). All were in current practice as of June 2013.

Mike Chapman, Electro-Mechanical Specialist, ASSA ABLOY / Architectural Security Group, Garland, TX

Scott Cheatham, Account Executive, ConTech CTI, Lubbock, TX

Richard Faught, Account Executive, Convergint Technologies, Oklahoma City, OK

Miles Fawcett, President, Urban Alarm, Washington DC

Patrick Fiel, Security Consultant, Wallace, NC

Doug Gambrell, Sales & Project Management, Safety-Technologies, Inc., Middleburg Heights, OH

Harry Gordee, CAT, Electronic Security, Tru-Lock & Security, Eau Claire, WI

Tom Hamilton, Designer, Security Electronics Inc., Lowell, OH

Steve Kaufer, CPP, President, Inter/Action Associates, Inc., Palm Springs, CA

Dorian Kruse, Engineered Systems Specialist, Capital Fire & Security, Inc., Madison, WI

Ron Lander, CPP, CMAS, PSM, Owner, Ultrasafe Security Specialists, Los Angeles, CA

Matt Lee, Account Executive, Convergint Technologies, Carrolton, TX

Tony Marquis, CEO, Homeland Safety Systems Inc., Shreveport, LA

Ray Rodríguez, Senior Security Consultant, Stanley Convergent Security Solutions, Houston, TX

Mike Simon, President, Stand Guard, Inc. / Connected Technologies, LLC, Crystal Lake, IL

Douglas Titus, CFM, Business Development Manager - Education, ASSA ABLOY / Door Security Solutions, New Haven, CT

Lloyd Young, Security Division Manager, API Systems Group, Inc., Tyler, TX

Industry Advisor: **David Koenig, CPP,** Partner, Capital Lock / Capital Fire & Security, Inc., Madison, WI

Project Manager: **Merlin Guilbeau,** CEO, Electronic Security Association, Irving, TX

Project Coordinator: **Virginia Williams,** Facilitator and Editor, Washington DC

Contributor Profiles

API Systems Group, Inc. *[integrator]* http://www.apisystemsgroup.com/

Lloyd Young is a security and fire alarm licensed systems integrator, and Private Investigator, with 31 years of experience in the electronic security industry.

ASSA ABLOY *[manufacturer]*
/ Door Security Solutions http://www.assaabloydss.com/en/local/dss/

Douglas Titus, CFM leads business development for the K-12 and university segments. He has extensive experience in the security industry, including facilities management, and has earned the Certified Facility Manager (CFM) accreditation from IFMA.

/ Architectural Security Group http://www.archsecurity.com/

Mike Chapman is a system support specialist with 25 years of experience in facilities management for education institutions, including physical security and safety audits, low voltage system design and implementation, and system training.

Capital Fire & Security, Inc. *[integrator]* http://www.capital-fire-security.com/

David Koenig, CPP is a security systems management professional with 33 years of experience in all aspects of security systems integration, design, installation, and services. He has served as a board member for several prominent security associations and has won several distinguished awards, including the 2012 Morris F. Weinstock Award for outstanding lifetime achievements.

Dorian Kruse is a system designer with 25 years of experience in the security industry, including consulting design and installation for several large commercial and educational institutions.

ConTech CTI *[integrator]* http://www.contech-cti.com/

Scott Cheatham is a risk and security management specialist with 20 years of experience in enterprise systems and holds several certifications and licenses. He provides IP security consulting and design for new construction and renovation, and oversees sales of networked security solutions.

Convergint Technologies *[integrator]* https://www.convergint.com/

Richard Faught is a system design specialist for access control and CCTV, with 13 years of experience in the security industry.

Matt Lee is an IP Video expert and owned an independent security company for 14 years prior to his current position with a national integrator.

Homeland Safety Systems Inc. *[integrator]* http://www.homelandsafetysystems.com/

Tony Marquis is the private owner of a regional security company, a system integrator with 27 years of experience, and active in advocating for state standards.

Independent Specialist *[consultant]* pvfiel@gmail.com

Patrick Fiel is a safety and security consultant with over 35 years of national experience managing security/law enforcement organizations, including schools, and advises on threat assessment, emergency preparedness, preventative design, and crisis recovery.

Inter/Action Associates *[consultant]* http://www.interactionassociatesinc.com/

Steve Kaufer, CPP is a security advisor and system designer with 40 years of experience, including owner of a regional security company, a contributing author to numerous security publications and research, and has maintained a current CPP certification since 1989.

Safety-Technologies, Inc. *[integrator]* http://www.safety-technologies.net/

Doug Gambrell is a project manager and systems specialist with 20 years of experience in fire, security, wireless technologies, and network applications, who has designed, estimated, installed and managed several hundred major projects for enterprise level institutions.

Security Electronics Inc. *[integrator]* http://www.security-electronics.com/

Tom Hamilton is a systems engineer with 39 years of experience designing security systems. He is licensed in several states to install, test and repair security systems, including fire alarm and sprinkler systems, and he is a licensed broadcast engineer.

Stand Guard, Inc. *[integrator]* http://www.standguardinc.com/
/ Connected Technologies, LLC *[remote web services]* http://www.connectedtechnologies.us/

Mike Simon is a security and energy management integrator with nearly 30 years of experience in the security industry, and a co-developer of a remote inter-system management platform

Stanley Convergent Security Solutions *[integrator]* http://www.stanleycss.com/

Ray Rodríguez is a senior system integrator with 35 years of experience in the security industry, specializing in school systems, anti-piracy systems and banking systems.

Tru-Lock & Security *[integrator]* http://www.tru-lock.com/

Harry Gordee, CAT is an electronic security specialist with 37 years of experience, including 30 years in Law Enforcement, and the last seven as an integrator in design and installation of physical security systems in schools and businesses.

Ultrasafe Security Specialists *[consultant]* http://www.ultra-safe.com/

Ron Lander, CPP, CMAS, PSM is a security, safety, and anti-terrorist specialist, with 40 years of experience in public safety and electronic security. He holds numerous certifications and awards and is active in several industry standards and legislative councils.

Urban Alarm *[integrator]* http://www.urbanalarm.com/

Miles Fawcett is the founder of a security company specializing in full building management and offsite support services, with extensive installations in the K-12 school system and similar institutions.

Electronic Security Association
6333 North State Highway 161, Suite 350
Irving, TX 75038

888.447.1689
www.ESAweb.org

