Aella Consulting Group, Inc.

Security Technology Consultants

White Paper:
An Overview of Physical Security Technology for Schools

What Security Technologies to Consider for Schools – Finding a Direction

Contents

The information contained in this document represents the current view of Aella Consulting Group on the issues discussed as of the date of this publication. Because Aella must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Aella, and Aella cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for information purposes only. Aella makes no warranties express, implied or statutory, as to the information presented in this white paper document.

Aella may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering subject matter in this document. All rights are reserved except as expressly provided in written license agreement from Aella. The furnishing of this document does not give you any license to these patents, trademarks, copyrights or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred.

If you have comments on this publication or would like additional information from Aella Consulting Group, please contact us at:
fjd@aellagroup.com

Purpose of This Document

This document is intended to introduce school practitioners to the various types of physical security technologies that should be considered for incorporation into their operational school security plans. The information we provide is intentionally high-level in order not to burden you with informational overload. This way you will be aware of the most commonly applied technical tools at your disposal before you commit to a specific direction.

Information beyond this high-level introduction is available in our book "A Primer on Electronic Security for Schools, Universities, & Institutions" and from thousands of security industry consultants listed at ConsultantRegistry.Org.

Overarching Concerns & Considerations

Security technology applied correctly can be a massive force multiplier[1], while saving you time and making your facility safer. There are important considerations you will want to keep in mind as you learn about applying these technologies:

Recent laws (passed & pending)

Between the horrific event of Newtown Connecticut and at the time of this writing, state legislatures introduced over 470 bills intended to improve school security. Not all of the introduced bills will become law, but the ones that do will need to be considered in your plans.

Some of the pending and signed bills focus on improving emergency response. Many of the security technologies described in this whitepaper can make emergency response more efficient when interfaced with other systems. For example, cameras in the area of the panic button can automatically display on a monitor and provide immediate insight to an area. Initially, you may have looked at installing cameras for other reasons and the panic button to protect staff, but the two systems work together when you plan well and consider all of the uses of your equipment in conjunction with your plan.

Mass Notification Regulations

Prior to the above noted legislative bills, NFPA 72 (which references ANSI/UL 2572) added requirements for Mass Notification that can apply to schools. Languages in new legislative bills reinforce, and sometimes duplicate, requirements found in NFPA 72. While not enforced uniformly nationwide, we recommend caution with regard to Mass Notification. This is because NFPA 72 has over-the-cliff (must be compliant with all requirements) verbiage that creates a liability for schools that attempt to "step into" mass notification.

[1] A force multiplier refers to something that increases (hence "multiplies") the effectiveness of an item, individual, or group. For example, a camera system can allow one security resource officer to monitor the front lobby and all the hallways at the same time.

Daily, Training, and Incident Modes

Another consideration is different modes of use. You may be adding technology like access control, so you do not have to post staff at every door during different parts of the day. That may be its intended primary function, but it may be helpful if that product also has a training mode or an incident mode like "Lock down".

Movies and Television Show Lie

Physical security technologies, like those that you see in the movies and television are not real. The technology often does not exist or is misrepresented in the effectiveness (It's Television for Entertainment). Most security industry "veterans" recognize the limitations of security hardware from years of exposure. Ask many questions when you evaluate technologies and do not overestimate what a system can do based on a fancy marketing presentation.

Does it play nice with IT?

Today, schools rely heavily on IT networks that are shared by hundreds of computers, Voice over IP desk phones, tablets, and a host of other connected devices. Physical security technology is yet another demand that schools are adding to their network infrastructure and network administrators.

Many of the physical security technologies you may want to add to a facility can be connected to the network. If not designed and implemented correctly, digital video surveillance systems can clog up a network to the point that nothing works. Likewise, other systems may require exacting data speeds or response times when communicating across your network.

Beyond the network, many of the security technologies you are considering implementing will have one or more computer servers which need a home. The obvious place to put these servers is with existing servers and in the capable hands of your IT team. Doing this takes up rack space, uses power, and adds heat.

In short, make sure to bring in your IT people early and keep them at your side.

New Cloud Service Options

Lately cloud computing has been garnering notoriety as more and more businesses take advantage of its benefits. This is also the case in the physical security market.
The costs of accessing security software through a cloud provider can offset the costs associated with purchasing and hosting software locally. However, online storage costs can be more restrictive versus what you can achieve under a onetime cost with local storage.

Just as every other decision, there are benefits and drawbacks to using cloud based physical security technologies. As you evaluate cloud service options, consider the following benefits and drawbacks:

Benefits –

Flexibility

The cloud promises and often delivers flexibility that can increase productivity and efficiency. Access to cloud based systems can be made through browsers on existing desktop and mobile devices.

Limited Maintenance

As with consumer and business cloud solutions, support and maintenance of software, servers, and storage devices is managed by the cloud service provider. Facilities with little or no on-site IT presence may find an acceptable solution using cloud services.

Drawbacks –

Limited Interfaces

Cloud based physical security technologies currently have limited interfaces to complimentary on-site or cloud based systems. This means the convenience and flexibility benefits of a cloud based access control solution may restrict your ability to interface with a video system.

Security

Security is paramount to your physical security technology plan. Can your cloud provider ensure the level of security that you require? Make sure to perform due diligence as part of your decision-making. In our security technology primer, we identified that a leader in consumer cloud storage was reported as having an application wide security incident due to employee error.

Internet connection/bandwidth

Uninterrupted access to your physical security system is crucial. Many of the cloud service providers offer high availability levels and high issue resolution response levels. However, the internet connection in between can be interrupted or slowed due to internet attacks. Even if you have a stable internet connection, the number of cameras your facility needs may demand more constant bandwidth than is available through your internet connection.

Data, Data, Everywhere!

A primary concern in designing the security system is how it will handle all of the associated information produced by the various physical security systems. For example:

- Alarms from the Intrusion & Fire Systems
- Alerts from the Access Control System
- Video from the Video Surveillance System

Recognize that each of these individual systems has evolved separately under different companies, and as a result, they present information differently. We will talk more about ways to control disparate data sources in the next section.

The rest of this whitepaper is dedicated to types of physical security technologies. As you continue reading and reflect on these technologies, consider whether they will meet the short and long-term needs of your facility and how you would want to access or see the information that these systems can deliver.

Physical Security Technologies

Tiered Technology Approach

There is no standard template for security technology that fits every application. In our primer [2], we refer to a "Tiered" method of constructing a physical security system. This proven method creates multiple hierarchal layers of physical security technologies, thereby delivering layers of autonomy, redundancy, and backup.

Physical Security Information Management (PSIM) / Command and Control

A well-designed, comprehensive security plan is not just about sensing and reporting alarms or recording and displaying video, it is about collecting and presenting all of the information in a coherent fashion so it can be effective used by security and safety personnel.

Physical Security Information Management (PSIM) systems, previously known as Command and Control, allow disparate information from differing manufacturers' products to become interoperable on a standard platform or "user interface". Most PSIM manufacturers are system agnostic; therefore most manufacturers do not see them as a competitor and will be willing to cooperate and work with them.

One of the major advantages of utilizing a PSIM is to provide a "big picture" or "situational awareness". This serves to provide everyday benefit, but can be extremely important in the most critical of emergency times. Most PSIM's can deliver additional benefit to the common operating picture with the ability to present a "live" campus system map. This map displays the systems in real-time, and the operational status of all the lower tier

[2] A Primer on Electronic Security for Schools, Universities and Institutions, 2nd Edition, March 2012.

systems using icons to indicate the status of doors, other sensors, cameras and other system attributes.

Smaller educational facilities may not warrant the addition and cost of a PSIM. However, PSIM is a good place to start our discussion because smaller, independent facilities are often brought into a campus wide plan.

On the following pages, we will talk about lower level systems that can function both independently or as Tier 2 systems under a PSIM.

Video Management Systems

On the surface, many Video Management Systems (VMS) look the same. At the most basic level, video management software products route and/or record compressed video from cameras and encoders, and display video to monitors. These systems also provide camera and user administration and access rights. Most of today's Video Management Systems (VMS) display live video in a graphical user interface (GUI) or a standard Windows internet browser on an operators PC. Some systems offer video "decoders" to display video directly on dedicated monitors or "video walls" without requiring a PC.

A close examination of available VMS reveals a wide variance of product features, functionality, and price. VMS manufacturers often times vary in maturity and market focus resulting in product differences in scalability, network management, fault tolerance, operating systems, software clients, and the availability of standard conventions and protocols (interfaces).

Video Management Systems require at a minimum: cameras, a PC platform with servers and storage equipment, and the manufacturer's software. Some manufacturer's designs are proprietary and require you to use their hardware, and/or software. Other manufacturer's feature more open designed platforms, which provide the opportunity for easier system additions and support.

You may hear references to CCTV, Digital Video, Video Surveillance, Security Cameras, and the 'mystical' Digital Video Analytics. We would like to point out that these terms are not interchangeable. Video surveillance is a rapidly changing segment of security that is much like computers, whatever you buy today will no longer be state of the art tomorrow. This rapid change and transitioning in the market (often referred to as "convergence") requires a well thought design concept to ensure the long-term viability of your installation.

Today, video surveillance is making a shift from analog cameras (based on the original one-signal-per-cable design) to network (IP) cameras (where many cameras can transmit on network cable). There are still many analog cameras being installed because integrators are comfortable with their installation and troubleshooting. However, they will be obsolete in the near future.

The key to extending the life of your video system is to install a platform that supports "open protocols". This term means that the purchaser will not be limited to proprietary technical components from a single vendor. In theory, future incremental enhancements then will be cost effective and take advantage of new technologies without having to incur sweeping replacement costs for major system components.

Cameras

Cameras are the most basic and critical element of video surveillance and predetermine operational characteristics of the entire system. The cameras you install predetermine certain system-wide operational characteristics such as:

- Fixed position or Pan/Tilt/Zoom (Can I remotely control the camera?)
- Standard resolution or megapixel (How wide of an area can I see or can I digitally zoom?)
- Built-in storage (Does video recording impact my network all the time?)
- Built-in video analytics (Do I get alarms from my camera that other systems can use?)
- Built-in processing power for future video analytics (Do I replace the camera or add hardware to use video analytics on a camera?)

Most recently, the cost for night vision and low light cameras has become economical enough to be used in commercial and educational applications to detect and capture images not previously available in older systems.

Monitors

Video surveillance monitors come in an assortment of sizes and technical functions. Monitors can be applied differently as your monitoring layout and overall design strategy requires. Many Video Management Systems utilize one or more flat panel monitors of larger size to view multiple images. Often VMS, Access Control, or PSIM's display additional system information, as well as video.

Multiple monitors maybe used, but you need to consider how your security personnel will use them. A good rule of thumb is that the more monitors security personnel are required to watch, the faster they develop monitor fatigue and are more likely to miss critical events. However, multiple monitors with important cameras displayed enable security personnel to assess critical areas at a glance.

Recording

Today's digital video recorders (DVR) and network video recorders (NVR) allow security system designers to use any combination of the previously discussed features of analog and IP security cameras.

DVR's are computers or purpose-built devices that use internal video capture hardware with specific channel capacities of 4, 8, 9, 16, 24, 32, and 64 (with each channel being a camera). These devices are closed ended with a predetermined storage size, thus requiring the need for additional devices if the system is expanded.

NVR's are designed to work with network edge devices (IP cameras and IP encoders) rather than directly connect with analog (non-IP) cameras. An NVR is a PC Server or specialized embedded device with video management software/firmware. NVR capacities vary substantially depending on the video management system and server specifications.

There are some hybrid recorders that offer both DVR (video capture hardware) and NVR (IP only), but they typically have a reduced total capacity of IP and analog video streams. Both DVR's and NVR's are easy concepts for IT directors and tech savvy consumers, but "build your own" is something to be avoided. "Build your own" is the practice of adding video capture cards and software to regular PC's and building your own DVR or NVR.

Recording systems vary tremendously in scalability (as we touch on above). Evaluation of camera types (standard vs. megapixel), calculation of the quantity of camera types, and the anticipated system growth must be considered carefully in your purchasing decision.

Analog, Digital, Standards Compliant?

Decisions regarding video systems invariably include decisions regarding analog cameras, digital cameras, or a combination of both. The differences are discussed later, but the important thing to know is that they use different wiring. Additionally, digital cameras can be proprietary (only work on one system), open standard (their communication standard is openly shared), or standards compliant (uses a communications standard promoted by an independent standards organization). Typically, the video management system you choose will limit your camera choices.

Digital Video Analytics

Though they have been around for some time, video analytics are still not well understood by all for the correct use and implementation. New advances and product offerings are available each year, but should be evaluated very carefully.

We are typically interested in video analytics as a way to monitor multiple cameras without concern for operator fatigue and to free up staff to do other things. However, video analytics have not progressed to the point where they can replace human decision-making or make judgment calls.

Typically Found Analytic Functions Include:

- Motion Detection
- Object Classification and Tracking
- Object Removed
- Object Left Behind
- Wrong way detection and object counting
- License Plate Detection
- Facial recognition

In every video analytics deployment, camera placement and properties have a profound effect on performance. Proper expectations and adequate design are critical to ensure a successful deployment.

Mass Notification Systems

The intent of Mass Notification Systems is as the name would imply, "to notify the masses" in the case of an event. Mass Notification type events can vary from the severe "a terrorist attack", to the informational, such as closings due to weather ("snow day").

As authors in this subject matter, we would be remiss not to caution the reader that Clery Act considerations and changes within NFPA, UL, and the D.O.E. set certain expectations and requirements regarding these systems. We advise that these items be given the consideration they deserve. Laws, regulations, and codes have begun to change regarding fire and notification systems. When designing these systems, NFPA & UL requirements and recommendations should be followed closely.

Many voice-based systems come preprogrammed with English, Spanish, or French messages, and often are able to use customized message(s) recorded by the customer. The power of the human voice added to the typical bell, siren, and flashing lights makes a system highly effective. However, too often systems are installed that are less than adequate, making annunciation of voice wholly unintelligible of which there are now established standards.

Mass Notification systems should include or consider the requirements unique to your setting as follows:

At a minimum:

- Public address system
- Posted notices
- Emergency call-in hotline
- SMS/Text messaging

- Website/portal
- Outdoor Public Address System/Warning Sirens
- Voicemail notification system
- Visually/Audibly impaired warning system

Recommended:

- Digital signage
- Desktop alerting in each classroom and throughout the campus/school
- Voice enabled programmable fire alarm
- Mobile loud speaker system(s)
- Blue light towers
- Staff radio system with alerting
- Outdoor emergency phones
- Utilization of Social media, blogs, etc.

This list is not all encompassing, but a starting point to identify and evoke the discussion regarding the responsibilities and the tools available in your unique circumstance to protect the students, faculty, and staff of the institution.

Access Control, Badging and Visitor Management

When access control is paired with visitor management and a badging system (credentials), the result is a more complete accounting and control of the entire school population. These systems should work in unison but not impair the functions of one another to create, access, or provide information.

Access Control

The purpose of an access control system is to limit access and create a record of accountability. Employees can only access areas where they are authorized, and during the times, they are authorized to be there. Likewise, students and visitors can be kept out of areas they are not supposed to access.

The most basic component of security access systems is a keypad or card reader or some combination of both located at entry points you wish to secure. The door access devices are wired to control panels and from there to a computer system (Server or other manufacturer specific PC) to run software. These panels are generally proprietary to the manufacturer. Access control systems typically allow the supplemental tie in and monitoring of multiple systems, i.e. fire, perimeter alarms, interior alarms, video system motion detection, and other alarms.

All access control manufacturers' software is proprietary, and therefore this decision is of paramount importance. Examine all of the performance details of the equipment to determine if, and how they meet your institutional requirements now, and for the future.

Badging System

Most mature access control systems have an integral badging system component allowing the creation of credentials (picture) on an access control card. However, the quantity and type of cards may dictate a badge product from a manufacturer that is different but integrated with the access system.

Card readers (credential readers) utilizing magnetic stripes, RFID technology, and traditional weigand swipe technology are the most prevalent access control device. RFID technologies include Prox (short for proximity) and smart cards, are similar to Prox, but house additional data other than just the user's ID.

As you evaluate these choices, you may be tempted to tie your cafeteria or other card based purchasing program (sometimes referred to the One Card system). Our experience is that combining the security and commerce is generally problematic because they are specialized.

Visitor Management

Visitor management in school is a valuable extension of a well-designed access control plan and is intended to let the right people in and keep the wrong people out. Software based visitor management systems can quickly verify visitor's credentials against a blacklist or a whitelist [a Criminal Offender Record Information (CORI) check is essential here] and provides an audit trail that is easy to create and access. Beyond the obvious security improvement, visitor management makes your entire staff accountable for visitors while on site.

Ties between the access control system and the visitor management system can aid in accountability if the building must be evacuated. Most robust Visitor Management systems can be used to determine the presence of visitors within the facility or provide a "muster list" to account for all evacuated guests.

Fire & Intrusion Central Monitoring

There are several ways to approach the monitoring of your security and fire alarms systems. Please keep in mind, as we have stated earlier, the best system designs incorporate layered redundancy, which in the case of fire and intrusion systems lends itself to supplemental monitoring by a hierarchal system.

All state of the art Fire and Intrusion systems contain digital communicators capable of transmitting to a central station or monitoring center in a variety of formats. However, you will have to make sure your systems support a format that is compatible with whatever central station or monitoring method, you elect to use.

In the conventional configurations, digital receivers are assigned to dedicated telephone lines and integrated with the central station software. Field security panels send alarms, open & closing signals, supervisory signals, and test signals of all systems to central station receivers. The central station software deciphers this information and displays it on computer terminals for action by the central station operator.

There is a growing segment of security systems equipment, which can be centrally monitored over the Internet. Only specific equipment has been listed or approved to date.

User Owned Central Station or Monitoring Center

There is a significant expense to operating your own central station. It is only reasonable to consider your own central station if you have your own police, fire, and security forces deployed 24 hours a day, seven days a week, and 365 days a year and are willing to hire fulltime dispatchers.

Independent Third Party Central Station

The third party central station will usually be UL approved, thereby providing all of the assurances of outside-unbiased supervision and having all of the electrical, physical, ventilation, and software requirements met. Third party central stations are in the business to provide this type of monitoring, so they assume all the burdens of insurance, training, and any licensing requirements.

This solution usually is best for the school, university, or institution that does not have a full time police or security officer program to mitigate all of the associated costs. It has the most flexibility with the least associated risk, and it provides some sharing of the risk and liability.

Security Supplier Owned Central Station

In some instances where a school district, university, or institution contracts their security services to a security systems supplier, including monitoring, it is the responsibility of the security systems supplier to assume all of the previously discussed burdens of cost, insurance, training, licensing, and UL approval.

Whichever monitoring solution you ultimately adopt, we strongly recommend that you do not rely solely on unsupervised telephone lines as your sole source of communications with the central station. We highly recommend that you employ backup solutions involving cellular communication back up, telemetry, long-range radio, or a network-deployed application to facilitate the delivery of emergency signals during telephone outages.

Intrusion Detection Systems

Intrusion Detection is an integral part of your physical security technology. Intrusion detection can be a standalone Intrusion Detection System (IDS), but is often part of an

Access Control System. The descriptions below apply to both types of applications of the technology.

IDS sensors (described below) are connected using dedicated wiring. This wiring is often protected in metal conduit to prevent tampering or rendering a device inoperable by simply cutting the wire. In many cases, these sensors will be "supervised" to detect tampering or make the sensors inoperable.

Rather than run wire from every device back to a central point, IDSs usually have control panels located throughout the building in secure locations. As with the device wiring, IDS panels should also be monitored for tampering.

Balanced Magnetic Contacts

Balanced contacts are used on all types of indoor and outdoor doors and windows to detect when opened or closed.

Motion Detection

The use of long-range combination passive infrared (PIR) and microwave detectors in corridors and hallways is commonplace. These represent two different technologies, which can be applied to detect motion in different areas. PIR measures infrared (IR) light radiating from objects in its field of view. While very accurate, these devices can create false alarms from items that change temperature such as heating radiators, and electronics.

Microwave detectors send out pulses of ultrasonic waves and measure the reflection off a moving object to detect motion. The technology works similar to a police radar gun. These devices are also very accurate but they can be bothered by electrical "noise".

Some motion detectors use a combination of both PIR and microware technologies; when the PIR sensor is tripped, it activates a microwave sensor to confirm the motion detection.

Other Alarm System Features

The security system can be used for a host of other supervisory tasks capable of alerting school personnel of potentially damaging events. Monitoring food storage temperatures in coolers and freezers, monitoring power outages and generator failure to start, HVAC Systems and in colder climates, boilers used for heating is a frequent application.

The security system can also be used to monitor the building fire alarm system (provided it meets the UL Laboratories listing).

In addition to the protection provided by the security systems, a well-documented deterrent is signage deployed throughout the facility identifying that these premises are monitored and protected.

Fire Alarm Systems

Fire alarm manufacturers are regulated and scrutinized by Underwriters Laboratories, National Fire Protection Association, Factory Mutual, insurance risk carriers, federal and state agencies, ADA, and many others. They are tested routinely in order to insure reliability. If they are so reliable, then what is the concern?

For fire alarm systems to be of any value, they must be designed, installed, and maintained correctly. If you already have a fire alarm system, the following information can help you to understand where you might lower some of your maintenance costs and how to integrate your fire system into your overall physical security plan.

Conventional Versus Addressable

Fire alarm architecture is described as conventional or addressable. Your choice of architecture determines the devices you can attach and some of your system's core functionality.
In both cases, there are two functional sides of a Fire Alarm System; Detection and Annunciation. The detection side of a fire alarm system is comprised of detectors and pull stations that are connected to a fire alarm panel. Similarly, the annunciation (or alarming) side of the system is comprised of the same fire alarm panel and is connected to strobe lights and alarm sounders.

Depending on local code and the fire alarm panel design, these zones may refer to an area of the building such as the "south hallway classrooms" or the "auditorium".

Fire Alarm Components

Smoke and heat detectors are your primary fire detection devices and should be installed according to code and located throughout the structure. Manual pull stations should also be located according to code and protected with covers that sound an audible alarm if the manual pull station cover is opened. This prevents false alarms and class disruption.

It is also important to remember all horn/strobes also must be located in compliance with the fire code, Authority Having Jurisdiction (AHJ), and Americans with Disabilities Act (ADA).

There are many types of fire detection devices on the market today and most do a great job for their intended area of specialization. There are also many mainstream and

specialized detectors available; we recommend that you follow code requirements when deciding which of them you need.

School Bus Security Technology

Technology has advanced rapidly to the point where it is economically feasible to track and provide two-way communication and private or public addressing to each school bus. This technology will handle an array of potential hazards that may be faced during the day while a bus is in transit. Video recording of events helps to deter and defend against bullying, assaults, and accidents.

In addition to the information that can be transmitted and gathered from the buses, this information can be utilized by state and local law enforcement, even in real time from a mobile platform. Hand-off of video and data from buses can be efficiently handled and coordinated to work in harmony with school security and notification.

Some important considerations that exist when presenting and detailing the need for the technology inclusion within your bus fleet are as follows:

- Is the technology designed for a mobile/transportation environment
- Hardened equipment with power backup
- Recording mechanisms that are hardened or solid state
- Protected from extremes of heat and cold
- Is the wireless technology incorporated in the hardware
- How are updates delivered to the hardware and software (directly or wirelessly)
- How does the system report faults
- Are the cameras designed for rigors of environment
- What other peripheral devices (lights, panic switches, geolocation) can be added to the system

Physical security technology on school buses and public transportation is currently a specialty niche serviced primarily by companies specializing in transportation. Only a few of these systems can interface with other physical security systems.

Our Summary

Physical Security Technology cannot and will not provide you with security in a school, but rather is part of a holistic approach and a well-crafted security and safety plan. Security technology applied correctly can be a huge force multiplier[3], while saving you time and making your facility safer.

This document was intended only to introduce you to the technologies that should be considered by school practitioners for incorporation into their operational school security plans.

The information we included was intentionally high-level to provide awareness of the most commonly applied technical tools at your disposal before you commit to a specific direction. We highly recommend that a multi-disciplinary team address the needs of your school to insure that you have all of the components of a complete security plan.

[3] A force multiplier refers to something that increases (hence "multiplies") the effectiveness of an item, individual, or group. For example, a camera system can allow one security resource officer to monitor the front lobby and all the hallways at the same time.

Appendices

Appendix A - Resources

- American Society for Industrial Security asisonline.org
- American Board for Certification in Homeland Security (ABCHS) abchs.com
- Construction Specifications Institute csi.net
- Consultant Registry ConsultantRegistry.Org
- InfraGard infragard.org
- International Association of Campus Law Enforcement Administrators iaclea.org
- National Fire Protection Association (NFPA) nfpa.org
- U.S. Department of Education (DOE) ed.gov
- U.S. Department of Homeland Security (DHS) dhs.gov
- U.S. Federal Emergency Management Agency (FEMA) fema.gov

Appendix B - References

A Primer on Electronic Security for Schools, Universities, & Institutions
schoolsecurityprimer.com

Appendix C - Authors

Frank J. Davies

Frank J. Davies is a veteran of 30 years in the physical and electronic security industry and is currently president and co-founder of Aella Consulting Group, Inc. Frank has specialized in the design development and implementation of sophisticated security integration projects for the Federal Government, Airports, Universities and Fortune 500 clientele.

Frank is a Certified in Homeland Security (CHS-IV) by the American Board for Certification in Homeland Security, a Certified Infrastructure Professional with the Office of Infrastructure Preparedness, • National Fire Protection Association (NFPA) Member, InfraGard Member (FBI Private/Business Organization), American Society for Industrial Security Member (Since 1984), and the International Association of Campus Law Enforcement Administrators (Since 1996) and remains active in all of these organizations.

Frank is recognized as a Physical Security Expert and is an active participant on the following councils and boards:
American Board for Certification in Homeland Security (ABCHS)
- Member ABCHS 2013 School Safety & Security Panel
American Society for Industrial Security (ASIS) member (since 1986)
-Member ASIS National School Safety & Security Council (2012, 2013)

Frank was educated at Syracuse University and The University of New Hampshire and holds a BA in Communications and continued studies through The Whittemore School of Business and Economics in pursuit of his MBA.

Gregory Bernardo

Greg Bernardo has held key positions for over 18 years in the physical and electronic security industry. His experience includes sales & marketing, technical support, applications design, product management, project management for various security industry leaders and is currently vice president and co-founder of Aella Consulting Group, Inc.

Greg has implemented sophisticated security integration projects for Healthcare facilities, K-12 Institutions of Education and Fortune 500 clientele. Greg has performed site surveys & security assessments, development of mitigation plans, systems design, bid project specification documentation, drafting, equipment and labor estimation and grant writing for some of the largest airports, seaports and school districts in the United States.

Greg is a Certified Documents Technologist (CDT) by The Construction Specifications Institute, Certified in Homeland Security (CHS-IV) by the American Board for Certification in Homeland Security, and has been a supporting member of the American Society for Industrial Security (ASIS) since 2004.

Greg is an active participant with the American Board for Certification in Homeland Security (ABCHS) and is the acting Chair for the ABCHS 2013 School Safety & Security Panel.

Additional Publications by the Authors

"A Primer on Electronic Security for Schools, Universities & Institutions"
2012 - Frank J. Davies, Gregory Bernardo, Henry Homrighaus.
schoolsecurityprimer.com

"White Paper: Mass Notification Requirements for Our Children's Schools"
2012 - Frank J. Davies, Gregory Bernardo
aellagroup.com

"White Paper: "You Get What You Pay For"□ or "When Free is Not Really Free" "
2013 - Frank J. Davies, Gregory Bernardo
aellagroup.com