U.S Department of Justice
Office of Justice Programs
National Institute of Justice

National Institute of Justice

Research Report

The Appropriate and Effective Use of Security Technologies in U.S. Schools

– Volume I –

(Version NS-I)

A Guide for Schools and Law Enforcement Agencies

U.S. Department of Justice
National Institute of Justice

U.S. Department of Education
Safe and Drug-Free Schools
Program

U.S. Department of Energy
Sandia National Laboratories

U.S. Department of Justice
Office of Justice Programs
810 Seventh Street N.W.
Washington, DC 20531

Janet Reno
Attorney General

Raymond C. Fisher
Associate Attorney General

Laurie Robinson
Assistant Attorney General

Noël Brennan
Deputy Assistant Attorney General

Jeremy Travis
Director, National Institute of Justice

Office of Justice Programs
World Wide Web Site
http://www.ojp.usdoj.gov

National Institute of Justice
World Wide Web Site
http://www.ojp.usdoj.gov/nij

The Appropriate and Effective Use of Security Technologies in U.S. Schools

A Guide for Schools and Law Enforcement Agencies

Mary W. Green
Sandia National Laboratories
September 1999

NCJ 178265

National Institute of Justice
Jeremy Travis
Director

Raymond Downs
Program Monitor

This project was supported under award number 97–IJ–R–072 from the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Justice.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, the Bureau of Justice Statistics, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

Foreword

Creating safe schools is the responsibility of the entire community in which a school or school system resides, but responsibility for maintaining them on a day-to-day basis lies principally with school administrators and, to a lesser extent, the local law enforcement agency. To assist schools in this task, the U.S. Department of Education and the U.S. Department of Justice have sponsored, often jointly, both research and demonstration programs to collect data and test useful new ideas that will expand understanding of school violence and disorder and lead to new programs to reduce these problems.

This document provides basic guidelines to law enforcement agencies and school administrators and encourages their collaboration as they decide what, if any, security technologies should be considered as they develop safe school strategies. In the wake of recent high-profile school tragedies with multiple homicides, many of this Nation's communities have urged their school districts to incorporate security technology into their safety programs. This guide should help schools, in concert with their law enforcement partners, analyze their vulnerability to violence, theft, and vandalism, and suggest possible technologies to address these problems in an effective manner. This guide describes existing commercially available technologies and urges thoughtful consideration of not only the potential safety benefits that may accrue from their use but also the costs that schools may incur for capital investments, site modifications, additional staffing, training, and equipment maintenance and repair.

Topic areas included in this guide are: security concepts and operational issues, video surveillance, weapons detection devices (walk-through and hand-held metal detectors and x-ray baggage scanners), entry controls, and duress alarms.

Though this document does not replace the use of appropriate expert advice or provide detailed instructions on installing equipment or making cost estimates, it does offer practical guidance that should enable schools and law enforcement agencies to make better informed decisions on security technology.

Safety and security technology can only be one tool in a comprehensive program that each school must develop to create a safe learning environment that is perceived to be safe by all students and staff.

Jeremy Travis
Director, National Institute of Justice
U.S. Department of Justice

Bill Modzeleski
Director, Safe and Drug-Free Schools Program
U. S. Department of Education

Preface

A team of security specialists from the Security Systems and Technologies Center at Sandia National Laboratories first talked with local schools in 1991. It was our intent to share what we had learned about the strengths and weaknesses of security technologies through our work with the U.S. Department of Energy (DOE) in many public schools.

After visiting some 120-plus schools across the country, completing our DOE-funded work to improve security at Belen High School in New Mexico and performing additional school security work for the National Institutes of Justice (NIJ), we have learned that school security, like security for other applications, is not simple and straightforward. We have learned a lot about the unique aspects of school security from the many students, parents, and school and law enforcement personnel we met during the course of our work. At any particular school, security is the product of funding, facilities, building age, building layout, administrators, teachers, parents, kids, personalities, campus order, security personnel, procedures, the neighborhood, policies, the school board, local law enforcement, fire codes, local government, politics, and reputation. No two schools will have identical and successful security programs—hence, a security solution for one school cannot just be replicated at other schools with complete success.

What did become clear after working with more than 100 schools during the past 7 years is that school administrators need a good information resource on technologies for physical security problems. This guidebook, *The Appropriate and Effective Use of Security Technologies in U.S. Schools,* is anticipated to be the first in a series of manuals designed and written for use by school administrators and law enforcement agencies. The goals of these documents are to provide nontechnical, nonvendor-specific information on:

- The kinds of security products available on the market.
- The strengths and weaknesses of these products and their expected effectiveness in a school environment.
- The costs of these products, including installation, long-term operational and maintenance expenses, manpower, and training.
- Requirements to include in Requests For Quotes (RFQs) to get a good product for an application.
- Legal issues that may need to be addressed.

Although security products can certainly have many different applications, this document covers products that can be applicable to some of the issues of violence in schools: video surveillance, weapon detection, entry control, and duress alarms. Future volumes are expected to cover issues and products such as bomb threats and explosives detection; drug residue and drug vapor detection; drug use detection; alcohol use detection; interior and exterior intrusion detection sensors; alarm communications; antigraffiti sealers; false fire alarm pulls; glass-break sensors; two-way radios; fencing; antitheft property marking; doors, locks, and key control; Crime Prevention Through Environmental Design (CPTED) principles; and parking lot safety. Most of the issues and philosophies covered in these manuals are geared toward middle schools and high schools, but elementary schools will likely find several of the technologies to have possible applications at their facilities.

Although this document addresses nontechnology measures that we felt were important for the completeness

of the topic, there are many good resources and references available that address these people/policy/procedure/program issues much better. See the Resources section at the back of this book.

Feedback from law enforcement agencies, schools, and product manufacturers/vendors is welcome, especially regarding any oversights or errors on our part. This guidebook is intended to provide an overview of security technology product areas that might be appropriate and affordable for school applications. Appropriate corrections or additions will be included in future updates. (We apologize if our cost estimates for hardware do not reflect current pricing; this document was written more than a year before actual publication.)

I would like to extend our deep appreciation to the many schools who have allowed us to visit them and to assess the security vulnerabilities of their facilities and operations (and to take photos of the good things on their campuses, as well as the bad). I never failed to learn something new at every school we have visited. I found there to be many great schools in this country, with very motivated and hard-working administrators giving 110 percent of their energies to keep their students safe. I was humbled by the intense and stressful hours they worked and the ultimate importance of their jobs.

My thanks to the National Institute of Justice (NIJ) for providing the funding to conduct the research that allowed me to prepare this guidebook. I hope that we have met the high standards NIJ has set for providing the best that science and technologies have to offer in fighting crime in the United States. I owe special gratitude to Dennis Miyoshi, Director of Sandia's Security Systems and Technologies Center; Dennis has always been an advocate for schools and was the greatest ally in accomplishing Sandia's school security work.

Information regarding the availability and ordering process for these manuals and any updates may be obtained at the NIJ Web site: *www.ojp.usdoj.gov/nij;* the Justice Technology Information Network (JUSTNET): *www.nlectc.org;* or by calling 1–800–248–2742.

I would be interested in hearing from readers regarding their successes, as well as their failures, in dealing with school security technology issues.

Mary W. Green
mgreen@sandia.gov
Sandia National Laboratories
Mail Stop 0782
P.O. Box 5800
Albuquerque, NM 87185

Since 1941, Sandia National Laboratories has been a U.S. Department of Energy facility whose primary mission is providing engineering support for the U.S. nuclear weapons program. For the past 30 years, the Security Technologies and Research Division at Sandia has been the principal provider of research, design, development, and testing of leading-edge technologies to solve physical security problems at high-risk U.S. facilities.

Today, the Sandia facility in Albuquerque, New Mexico, employs more than 8,000 scientists, engineers, mathematicians, technicians, and support personnel to provide service in the national interest. More than 150 of these personnel are dedicated solely to research and development of security technologies.

Acknowledgments

Written by:	Mary W. Green, Sandia National Laboratories, Albuquerque, New Mexico
Original art work by:	Steven Scatliffe, Tech Reps, Inc., Albuquerque, New Mexico
Photos by:	George Wagner, Sandia National Laboratories, Albuquerque, New Mexico Steven Scatliffe, Tech Reps, Inc., Albuquerque, New Mexico
Document preparation:	Rosanne C. Rohac, Tech Reps, Inc., Albuquerque, New Mexico Elaine Perea, Tech Reps, Inc., Albuquerque, New Mexico
Additional contributors:	Janet Ahrens, Sandia National Laboratories, Albuquerque, New Mexico Tim Malone, Sandia National Laboratories, Albuquerque, New Mexico Dale Murray, Sandia National Laboratories, Albuquerque, New Mexico Charles Ringler, Sandia National Laboratories, Albuquerque, New Mexico George Wagner, Sandia National Laboratories, Albuquerque, New Mexico Fred Wolfenbarger, Sandia National Laboratories, Albuquerque, New Mexico
Library research:	Kay Kelly, BEI, Albuquerque, New Mexico
Reviewers:	Raymond Downs, Program Manager, National Institute of Justice William Modzeleski, Director, Safe and Drug-Free Schools Program, U.S. Department of Education Joe N. Anderson, Director of School Safety and Security, Metropolitan Nashville Public Schools Michael S. Ganio, Sr. Manager, Security Services, Orange County Public Schools John J. McLees, Executive Director, Philadelphia Office for School Safety Tom Hall, School Police Chief, San Diego Unified School District Kenneth Trump, President and CEO, National School Safety and Security Services Gary Underwood, Chief, San Bernardino Police, School Safety Department Paul Schultz, Chief of Police, LaVista Police, LaVista, Nebraska Ronald Sloan, Chief of Police, Arvada Police Department, Arvada, Colorado John C. Martinez, Deputy Chief, Dallas Police Department J.M. Hutt, Sergeant Arapahoe County Sheriff's Office, Englewood, Colorado Tod Schneider, Crime Prevention Specialist, Police Services Division, Eugene, Oregon Ed Hardy, Chief, Special Investigative Unit, Broward County School District, Sunrise, Florida Donovon Collins, Chief, Dallas Independent School District Police Mel Seo, Auxiliary Service Specialist, Hawaii Department of Education Jack Lazzarotto, Director, Police Services, Clark County School District, Las Vegas, Nevada Charles Clark, Director, Security Emergency Preparedness, Long Beach Unified School District Wesley Mitchell, Chief, Los Angeles School Police Sharon O'Connor, Tech Reps, Inc., Albuquerque, New Mexico

Contents

Pearl High School, Pearl, Mississippi

Chapter I The Big Picture: Security Concepts and Operational Issues

Most schools in the United States are safe institutions, with disciplinary issues creating most disruptions. However, because of the 1998 campus slayings involving students, firearms, and multiple victims, schools and school programs are working harder to reach out to students, to teach them to be good citizens, to identify potentially dangerous personalities, and to develop appropriate intervention strategies. There are many excellent programs around the country that address the issues of bullying, anger, hate, abuse, drugs, alcohol, gangs, lack of role models, vandalism, and so forth. It is of great importance to the United States that these programs be pursued expeditiously. Unfortunately, these programs cannot be successful overnight (indeed, many must be initiated early in a child's life in order to be most effective) and do not yet exist in all schools. Meanwhile, security incidents are occurring in schools that must be dealt with now—perpetrators must be caught and consequences must be administered. School administrators would like to discourage security infractions by means of any deterrent available to them. One such approach sought more often today involves security technologies.

Security technologies are not the answer to all school security problems. However, many security products (e.g., cameras, sensors, and so forth) can be excellent tools if applied appropriately. They can provide school administrators or security officials with information that would not otherwise be available, free up manpower for more appropriate work, or be used to perform mundane tasks. Sometimes they can save a school money (compared to the long-term cost of personnel or the cost impact of not preventing a particular incident). Too often, though, these technologies are not applied appropriately in schools, are expected to do more than they are capable of, or are not well maintained after initial installation. In these cases, technologies are certainly not cost effective.

Why security technologies?

To reduce problems of crime or violence in schools: (1) the opportunities for security infractions should be eliminated or made more difficult to accomplish, (2) the likelihood of being caught must be greatly increased, and (3) consequences must be established and enforced. Item 3 is a social and political issue and needs to be addressed head on by school boards and communities across the country. This guide addresses only items 1 and 2.

Simply providing more adults, especially parents, in schools will reduce the opportunities for security infractions and increase the likelihood of being caught. However, adding dedicated professional security staff to perform very routine security functions has many limitations:

- Locating qualified people may be difficult.
- Humans do not do mundane tasks well.
- Manpower costs are always increasing.
- Turnover of security personnel can be detrimental to a security program.
- As in other security environments, more repetitious tasks become boring.

Hence, the possible role of security technologies expands. Through technology, a school can introduce ways to collect information or enforce procedures and rules that it would not be able to afford or rely on security personnel to do.

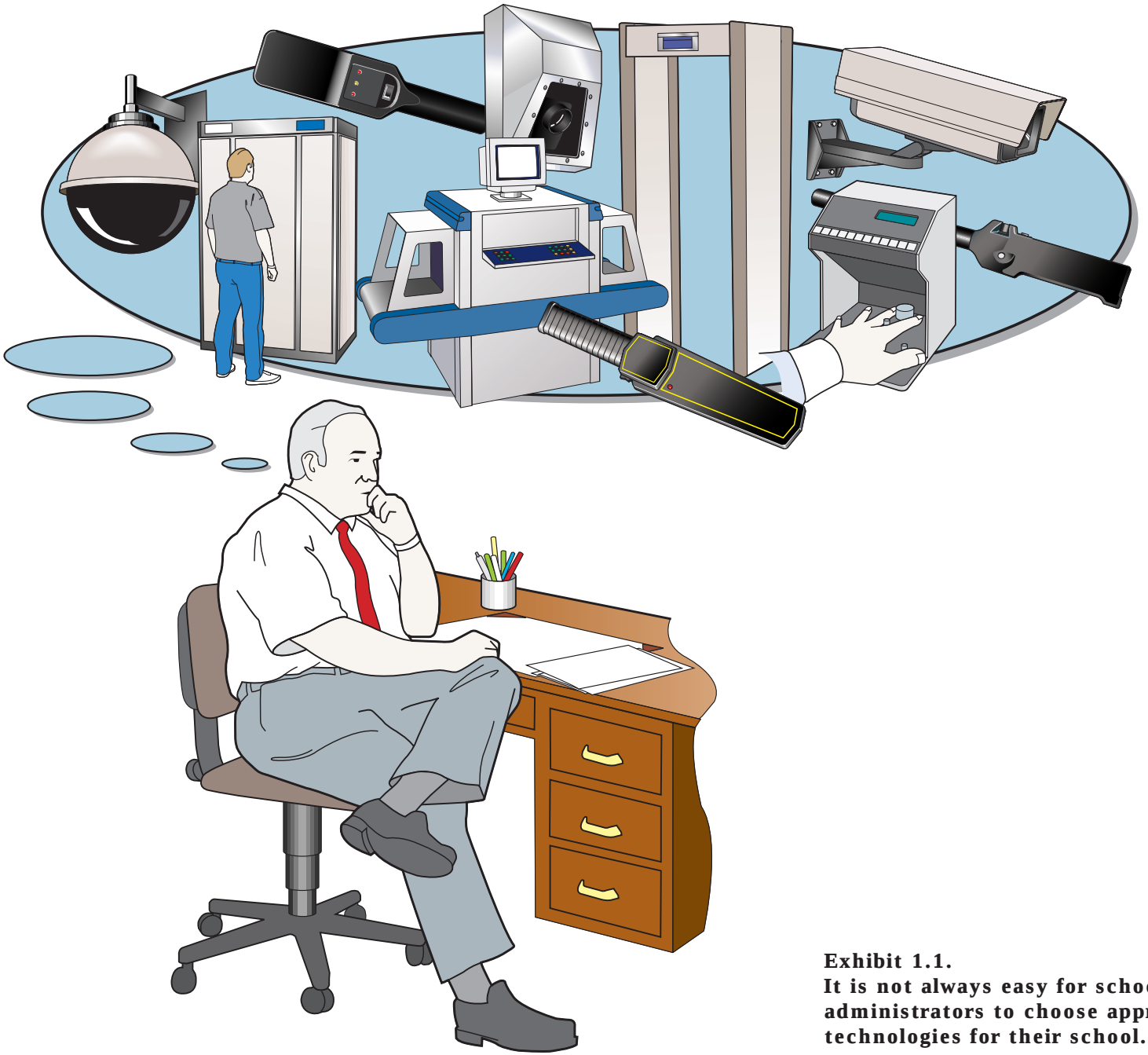


Exhibit 1.1.
It is not always easy for school administrators to choose appropriate technologies for their school.

Why security technologies have not been embraced by schools in the past

Anyone working in the security field is aware that there are thousands of security products on the market. Some of them are excellent, but many claim to be "the very best of its kind." And, unfortunately, there are a significant number of customers in the country who have been less than pleased with the ultimate cost, maintenance requirements, and effectiveness of security technologies they have purchased. Schools have been no exception to this and have a few inherent problems of their own:

- Schools do not usually have the funding for aggressive and complete security programs.
- Schools generally lack the ability to procure effective security technology products and services at the lowest bid.
- Many school security programs cannot afford to hire well-trained security personnel.
- School administrators and their staff rarely have training or experience in security technologies.
- Schools have no infrastructures in place for maintaining or upgrading security devices—when something breaks, it is often difficult to have it repaired or replaced.
- Issues of privacy and potential civil rights lawsuits may prohibit or complicate the use of some technologies.

The issues come down to applying security technologies in schools that are effective, affordable, and politically acceptable but still useful within these difficult constraints.

Effectiveness versus affordability versus acceptability

Effectiveness, affordability, and acceptability are difficult tradeoffs and, occasionally, a seemingly ineffective solution to a security problem is chosen because of a lack of funding or pressure from the community to do something.

Arguments often used against security initiatives:	**Some counter-arguments:**
• "We've never done it that way before." →	• "We need to evolve our security strategies to keep up with the changing times."
• "This is a knee-jerk reaction." →	• "This solution will take care of the immediate threat while longer term social programs are put into place."
• "Our school will look like a prison." →	• "Our school will look like it is well controlled."
• "Students' rights may be infringed upon." →	• "Students have a right to a safe and secure school environment."
• "People will think we have a bad school," →	• "We will gain a reputation for controlling our problems."
• "We may be sued." →	• "We may be sued if we don't take this action."

Although many effective security measures are too expensive for schools, cost alone is not often the ultimate driver. Most major changes to security policies, including the introduction of technologies, are often brought on not by foresight but as a response to some undesirable incident.

This is not to say that a good argument should be made for applying every physical security approach in every school. "Appropriate" preparation is, by far, the greater "art" in security system design, and it includes an evolving plan, beginning with defining a particular school's risks.

A systematic approach to identifying the security risks at a school

Note: The following discussion considers all security risks to schools—violence, drugs, theft, and vandalism—not just those that may be addressed by the technologies covered in this volume. Depending on the acceptance and demand for this guide, future additional volumes will address the remaining technologies in greater detail.

In the past, schools have rarely understood the need or had the time or resources to consider their security plans from a systems perspective—looking at the big picture of what they are trying to achieve in order to arrive at the optimal security strategy. A school's security staff must understand what it is trying to protect (people and/or high-value assets), who it is trying to protect against (the threats), and the general environment and constraints that it must work within—the characterization of the facility. This understanding will allow a school to define its greatest and/or most likely risks so that its security strategy consciously addresses those risks. This strategy will likely include some combination of technologies, personnel, and procedures that do the best possible job of solving the school's problems within its financial, logistical, and political constraints.

Why is this careful identification of risk important? Because few facilities, especially schools, can afford a security program that protects against all possible incidents.

No two schools are alike and, therefore, there is no single approach to security that will work ideally for all schools. From year to year, even, a school's security strategy will need revision because the world around it and the people inside it will always be changing.

Defining a school's assets. For this school year, what is most at risk? The protection of the students and staff is always at the top of this list, but the measures taken to protect them will usually be driven by the defined threats. Are the instruments in the band hall very attractive targets for theft or vandalism? Is the new computer lab full of the best and most easily resold computers? Though desirable, a school cannot possibly afford to protect everything to the same level of confidence.

Defining a school's threats. For this school year, who or what is your school threatened by? Gang rivalries? Fights behind the gym? Drugs hidden in lockers? Guns brought to school? Outsiders on campus? Drinking at lunchtime? Vehicle breakins? Graffiti in the bathrooms? Accidents in the parking lot? How sophisticated (knowledgeable of their task of malevolence) or motivated (willing to risk being caught or injured) do the perpetrators seem to be? Measures taken to protect against these threats are driven by the characterization of the facility and its surroundings as mentioned earlier.

Characterizing a school's environment. Any security strategy must incorporate the constraints of the facility so that all strengths, weaknesses, and idiosyncrasies are realized and provided for. How risks are approached will largely be driven by facility constraints. If theft and vandalism are primary risks for your school, answers to questions regarding the physical plant will determine the optimal security measures. Is the school new or old? Are the windows particularly vulnerable? Does everyone who ever worked at the school still have keys? What is the nighttime lighting like? Does the interior intrusion sensor system work well, or do the local police ignore the alarms due to a high false-alarm rate? Are visitors forced or merely requested to go through the front office before accessing the rest of the school?

If outsiders on campus are a primary concern, it will be necessary to recognize the facility's ability to control unauthorized access. How many entry points are there into the buildings? Are gangs present in the area? Are the school grounds open and accessible to anyone, or do fences or buildings restrict access (exhibit 1.2)? Is there easy access to the school roof? Where are hiding places within the building or on the premises? Is the student population small enough so that most of the staff would recognize most of the students and parents?

If issues of violence are a major concern, a thorough understanding of employees, student profiles, and neighborhood characteristics will be necessary. What is the crime rate in the neighborhood? Is the school administration well liked by the students? Are teachers allowed access to the school at night? Are students allowed off campus at lunch time? How much spending money do students generally have? Are popular hangouts for young people close by and, for business establishments, does management collaborate with the school? Are expelled or suspended students sent home or to an alternative school? How many incidents of violence have occurred at the school over the past 4 years? What is the general reputation of the school, and how does it appear to an outsider? Are your most vocal parents prosecurity or proprivacy? Do your students like and respect your security personnel well enough to pass them pieces of information regarding security concerns? Once the school's threats, assets, and environmental constraints are understood, the security needs can be prioritized such that the school's security goals are understood by all those involved.

Identifying security needs and then securing the funding to pay for them are usually unrelated at most schools. Schools have to have a "Plan B," for program design which may be the perfect "Plan A"—but spread out over several years of implementation. If the desirable strategies (e.g., fencing, sensors, locker searches, speed bumps) are too costly or unpalatable to the community, a school may then need to modify the facility constraints (e.g., back entrances locked from the outside, no open campus for students, no teacher access after 10 p.m., all computer equipment bolted down, no lockers for students, and so forth).

Most school districts or school boards will be more supportive of security measures and the requested funding if they are well educated about the most likely risks faced each year and the options available. A security staff should not have the wide-open charter to "keep everything and everybody safe." A school board should be briefed as often as once a month as to what the current security goals are and what strategies are recommended, realizing that these will and must continue to evolve. If a school board member is clearly aware of a school's most important concerns and what

Exhibit 1.2. A 3-foot fence added very little security to this school that was constantly being vandalized.

is required to achieve them, then he or she is less likely to be swayed by an irate parent into making a decision that will handicap reasonable security efforts.

Designing the school security system

After identifying the risks or concerns at a noneducational facility, a methodical approach to the security plan would then examine possible solutions to each area of vulnerability from the perspective of:

Detection → *Delay* → *Response*

For any problem, it is necessary first to detect that an incident or problem is occurring. For example, when someone is breaking into a building, it is necessary that this act be detected and that information be supplied to the authorities as soon as possible. Next, this adversary must be delayed as long as possible so that the response force may arrive. A simple example of delay would be firmly bolting computer components onto large heavy desks, so that a thief is forced to use more time removing the bolts. Finally, someone, such as the police, must respond to the incident to catch the thief redhanded.

For a school environment, it is probably more appropriate to expand this model:

Deterrence → *Detection* → *Delay* →
Response/Investigation → *Consequences*

See exhibit 1.3 for more detail.

The most appealing step in any school security system should be to convince the perpetrator that he or she should not do whatever it is he or she is considering, whether the action is perceived as too difficult, not worthwhile, or the chances of being caught are quite high. Clearly, most security measures employed in facilities are intended for the precise purpose of deterrence, whether it be to discourage a thief, a drug dealer, or an errant employee. (Note: Deterrence is not generally considered part of the security strategy for most high-risk government facilities; this is due in part to the fact that quite a bit of deterrence comes "free" with other security measures, and it would be difficult to attribute a lack of security problems to any particular deterrence effort.)

Unlike other facilities, where a perpetrator would be handed over to the authorities, and the consequences determined by law, a school often has the authority and/or opportunity to establish the consequences for incidents that occur on their campus. It is imperative, however, that schools do not assume authority that they do not have. Issues governed by law must be reported to the appropriate authority.

To illustrate the application of this model, consider the problem of nighttime breakins and theft in a school building. A model for the security strategy to address this might be:

Deterrence	Close off the parking lot or driveways to vehicle traffic at night. Post signs that video cameras are in use on the campus (but only if you actually do have cameras). Use fencing strategically, but where fencing would be unacceptable, consider a barrier of thorny pyracantha bushes (exhibit 1.4). Allow a law enforcement officer to live on campus.
Detection	Install an intrusion detection system in all school hallways, administrative offices, and rooms with high-value

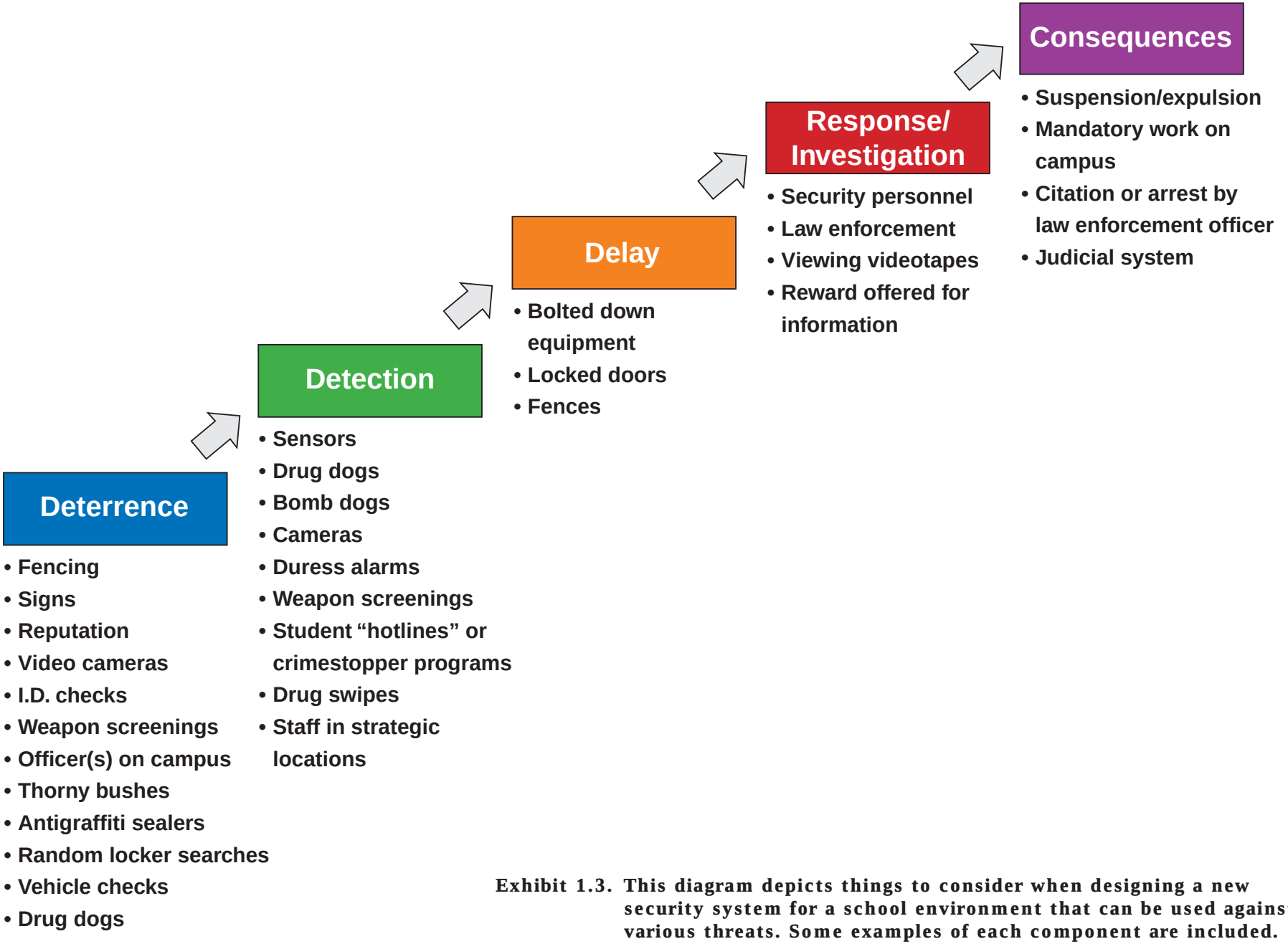


Exhibit 1.3. This diagram depicts things to consider when designing a new security system for a school environment that can be used against various threats. Some examples of each component are included.

Exhibit 1.4. Pyracantha bushes can create an intimidating barrier where fences might be inappropriate. Caution may be advisable as to the location of bushes so that convenient hiding places for contraband are not created.

	assets. Use motion sensors, magnetic switches on doors, heat sensors, and/or glass-break sensors as appropriate. Send alarm signals to the police, the officer on campus, and the school principal.
Delay	Bolt computers and TVs to desks and walls so that removing them is difficult and time consuming.
Response/ Investigation	Police and/or campus security arrives on the scene, makes arrests.
Consequences	Enforce consequences where possible and the school has the authority to do so. (This becomes an additional deterrent for the future, especially if nonsensitive pieces of information regarding the incident are released to staff, students, and the community.)

Schools do not normally have the opportunity for real-time detection and real-time response to security incidents; after-the-fact investigation is normally the best a school can hope for.

Although this model may not be appropriate for all aspects of security at a school, it can serve as a methodology for consideration. Its use can prevent some less-thought-out strategies. A true example of this is a large urban high school that was planning to purchase $100,000 worth of exterior cameras to combat nighttime vandalism being inflicted on the exterior of the building. This plan was halted abruptly when the school was asked who would be available to watch the monitors from the 40-plus cameras (detection) and who would be able to respond quickly enough to these sporadic and relatively small incidents (response). A better and cheaper alternate plan was devised that included using anti-graffiti sealer on all brick surfaces, some strategically located wrought iron fencing that could not easily be climbed, and the replacement of a few particularly vulnerable windows with glass block.

A spectrum of physical security approaches

It will be assumed that consequences for undesirable actions have been put into place at a school; otherwise, there is little or no deterrence to be gained from any physical security measures designed to detect, delay, and respond to an incident. A wide array of security measures involving people, campus modifications, and/or technologies can be considered for most concerns, keeping in mind the unique characteristics of each school. A recurring message from school administrators is that the majority of their problems are brought onto campus by outsiders or expelled/suspended students so measures to keep outsiders off campus will generally be of global benefit. (Although this is not the case in all incidents, school administrators quite often find it more palatable to parents if security measures are justified based on the exterior threat rather than the suspicion of their children.) The following is a partial list of possible security measures to address various security issues:

(Most of the following suggested security measures are in use in one or more U.S. schools, but a few may not yet have been attempted. In any case, there is no comprehensive body of knowledge regarding their effectiveness. More research is needed to get a national picture on particular technologies. Also keep in mind that a school should always contact its legal counsel before participating in any new security program that involves searching or testing of people or property.)

Outsiders on campus

- Posted signs regarding penalties for trespassing.
- Enclosed campus (fencing).
- Guard at main entry gate to campus.
- Greeters in strategic locations.
- Student I.D.s or badges.
- Vehicle parking stickers.
- Uniforms or dress codes.
- Exterior doors locked from the outside.
- A challenge procedure for anyone out of class.
- Cameras in remote locations.
- School laid out so all visitors must pass through front office.
- Temporary "fading" badges issued to all visitors.

Fights on campus

- Cameras.
- Duress alarms.
- Whistles.

Vandalism

- Graffiti-resistant sealers.
- Glass-break sensors.
- Aesthetically pleasing wall murals (these usually are not hit by graffiti).
- Law enforcement officers living on campus.
- 8-foot fencing.
- Well-lit campus at night.

Theft

- Interior intrusion detection sensors.
- Property marking (including microdots) to deter theft.
- Bars on windows.
- Reinforced doors.
- Elimination of access points up to rooftops (exhibit 1.5).
- Cameras.
- Doors with hingepins on secure side.
- Bolting down computers and TVs.
- Locating high-value assets in interior rooms.
- Key control.
- Biometric entry into rooms with high-value assets.
- Law enforcement officer living on campus.

Drugs

- Drug detection swipes.
- Hair analysis kits for drug use detection (intended for parental application).
- Drug dogs.
- Removal of lockers.
- Random searches.
- Vapor detection of drugs.

Alcohol

- No open campus at lunch.
- Breathalyzer® test equipment.
- No access to vehicles.
- No lockers.
- Clear or open mesh backpacks.
- Saliva test kits.

Weapons

- Walk-through metal detectors.
- Hand-held metal detectors.
- Vapor detection of gun powder.
- Crimestopper hotline with rewards for information.
- Gunpowder detection swipes.
- Random locker, backpack, and vehicle searches.
- X-ray inspection of bookbags and purses.

Malicious acts

- Setback of all school buildings from vehicle areas (exhibit 1.6).
- Inaccessibility of air intake and water source.

Exhibit 1.5. Be aware that exposed utility conduits or drain pipes can allow easy access to a school's roof, creating an opportunity for theft, as well as a liability concern.

Exhibit 1.6. A school building's lack of setback from roads or parking areas can create vulnerability to an out-of-control vehicle.

- All adults on campus required to have a badge.
- Vehicle barriers near main entries and student gathering areas.

Parking lot problems
- Cameras.
- Parking decals.
- Fencing.
- Card I.D. systems for parking lot entry.
- Parking lots sectioned off for different student schedules.
- Sensors in parking areas that should have no access during schoolday.
- Roving guards.
- Bike patrol.

False fire alarms
- Sophisticated alarm systems that allow assessment of alarms (and cancellation if false) before they become audible.
- Boxes installed over alarm pulls that alarm locally (screamer boxes).

Bomb threats
- Caller I.D. on phone system.
- Crimestopper program with big rewards for information.
- Recording all phone calls, with a message regarding this at the beginning of each incoming call.
- All incoming calls routed through a district office.
- Phone company support.
- No pay phones on campus.
- Policy to extend the school year when plagued with bomb threats and subsequent evacuations.

Bus problems
- Video cameras and recorders within enclosures on buses.
- I.D.s required to get on school buses.
- Security aides on buses.
- Smaller buses.
- Duress alarm system or radios for bus drivers.

Teacher safety
- Duress alarms.
- Roving patrols.
- Classroom doors left open during class.
- Cameras in black boxes in classrooms.
- Controlled access to classroom areas.

Legal issues

Within each section of this manual, some legal issues have been noted regarding the use of various technologies. A reasonable approach to using any new security device would include checking with your legal organization, talking to schools in the area that have already implemented the measure, and inviting local law enforcement to come in to discuss the device's possible use. Although every possible ramification cannot be foreseen, it does help to be aware of issues that might be raised and to be aware of current thinking about ways to address each of these.

Evaluating a school's security system design

The staff assigned to handle security concerns should plan to meet on a regular basis for collaboration on new problems, needed changes to existing approaches, and the exchange of information and intelligence. New problems and proposed solutions may sometimes be presented (where appropriate) to school employees, the student council, the parent advisory group, the local police, or other schools in the area. Although including more people may lengthen the decisionmaking process,

making representatives of these groups a part of the security upgrade team for issues that would involve them will ensure buy-in. A side benefit will be that word will spread throughout the community that the school is taking active security measures, which will act as a deterrent.

New school design

Many school buildings in the United States have been constructed to achieve an inviting and open-to-the-community feeling, with multiple buildings, big windows, multiple entrances and exits, and many opportunities for privacy. Needless to say, these layouts are not conducive to many current requirements to address security needs. To combat broken windows and nighttime thefts, the country also went through a brief period of designing schools with almost no windows; the cavelike results these designs produced were soon found to be objectionable to many people.

Incorporating the principles of Crime Prevention Through Environmental Design (CPTED) in the design or remodeling of a school can contribute greatly to the control and security of the campus. There are several good sources of CPTED literature available through the Web; CPTED as applied specifically to schools will be covered in a subsequent volume.

If a district has the luxury of looking forward to a new school in the future, it is imperative that trained security personnel, who are familiar with the area and the community, and who will be responsible for day-to-day security operations in the new facility, are involved in every step of the new design. This is critical to ensuring that the design of the new school minimizes vulnerabilities. There are architectural firms specializing in schools that incorporate good security principles; a security-conscious design can actually help compensate in the long term for tight security budgets, fewer security personnel, and less sophisticated security gadgets. The following are some suggestions to keep in mind for a new facility; the funding, location, geography, streets, and neighborhood will usually drive which ideas are feasible for each new school. Although this list includes only a few basic security technologies (such as cameras, sensors, and so forth), the facility design should not preclude their straightforward installation in the future.

- Limit the number of buildings—one building is best—to limit outsiders on the campus.
- Minimize the entrances to the school building—having one or two main entrances/exits will support efforts to keep outsiders off campus. Allow enough room at the main entry in the event that a screening area (i.e., for weapon or drug detection) needs to be incorporated later on. Alarm other exits for emergency use only.
- Minimize the line of sight from secluded off-campus sites onto student gathering areas, the main entry doors, playgrounds, patios, and so forth (exhibit 1.7). (This suggestion must be tempered against the benefits gained from the natural, desirable surveillance by neighbors, passers-by, officers on patrol, and so forth)
- Allow for a security person to be posted at a single entrance onto campus to challenge each vehicle for identification of all occupants. Buses and school employees should have a separate (and controlled) entrance.
- Provide a dropoff/pickup lane for buses only.
- Minimize the number of driveways or parking lots that students will have to walk across to get to the school building.

Exhibit 1.7. The administrators of this rural western school were concerned about their susceptibility to firearms due to the geography of their campus. A nontechnical but workable solution for this school was to allow local police officers to relocate their personal house trailers to strategic locations on campus to deter would-be snipers.

- Build single-stall bathrooms to mitigate bathroom confrontations and problems.
- Enclose the campus. (This is more a measure to keep outsiders out rather than to keep insiders in.) Beside defining property boundaries, a robust fence forces a perpetrator to consciously trespass, rather than allowing casual entry.
- Make certain that the school building and classroom areas can be closed and locked off from the gym and other facilities used during off hours.
- Minimize secluded hiding places for unauthorized persons, both inside and outside buildings.
- Do not eliminate windows, but use them strategically. Consider incorporating clerestories or secure skylights that allow light in but that are less vulnerable than typical windows.
- Maximize the line of sight within buildings.
- Large wide spaces, like hallways or commons, should have sufficient vertical dimension so space does not feel restrictive to students.
- Consider installing student lockers in classrooms or other areas easy to monitor so that there is no single locker area that becomes a bottleneck, and there is always the deterrence of an adult nearby (exhibit 1.8).
- Do not cut corners on communications, especially those required for security. Make certain that your facility has built in the necessary receivers and transmitters throughout the structure to allow for dependable two-way radio and cellular phone use. (Sometimes radio frequency communication is not possible deep within a large, structurally dense facility.)
- Where possible, have buildings and other student gathering areas set back from the streets, driveways, or parking areas by at least 50 feet.
- Install a basic security alarm system throughout all hallways, administrative offices, and rooms containing high-value property, such as computers, VCRs, shop equipment, laboratory supplies, and musical instruments.
- Allow a law enforcement officer to live on campus. (In some school districts, an officer is allowed to move his or her own trailer to a strategic location on campus and receive free utilities in exchange for prenegotiated and formally contracted responsibilities.) The deterrent effect of a police vehicle parked on campus all night and weekend can be great. Such an arrangement can also provide both detection and response in situations where damage is being inflicted upon the facility, but no alarm system would normally detect it (exhibit 1.9).
- Provide a separate parking area for work-study students or those who will be leaving during the school day. (This allows the main student parking lot to be closed off during the school day.)
- Make certain that exterior lighting is sufficient for safety. Lights mounted on the exterior of buildings often are inadequate for adjoining driveways or parking lots.
- Do not underestimate the value of trees and landscaping on a school campus. An attractive, well-maintained school is generally less attractive to thieves.

Exhibit 1.10 shows a school with several of these ideas incorporated. (Note: This is not an actual architectural drawing, does not incorporate basic facility requirements, and is not drawn to scale.)

The role of order maintenance

One additional consideration that cannot be overlooked is the perception of a lack of order on a school campus.

Exhibit 1.8. Cramped locker bays are some schools' most vulnerable area for fights, theft, drug deals, and so forth.

Exhibit 1.9. Will anyone be aware of malicious activities occurring at your school during off hours? This senior "prank" destroyed more than 20 trees at this high school.

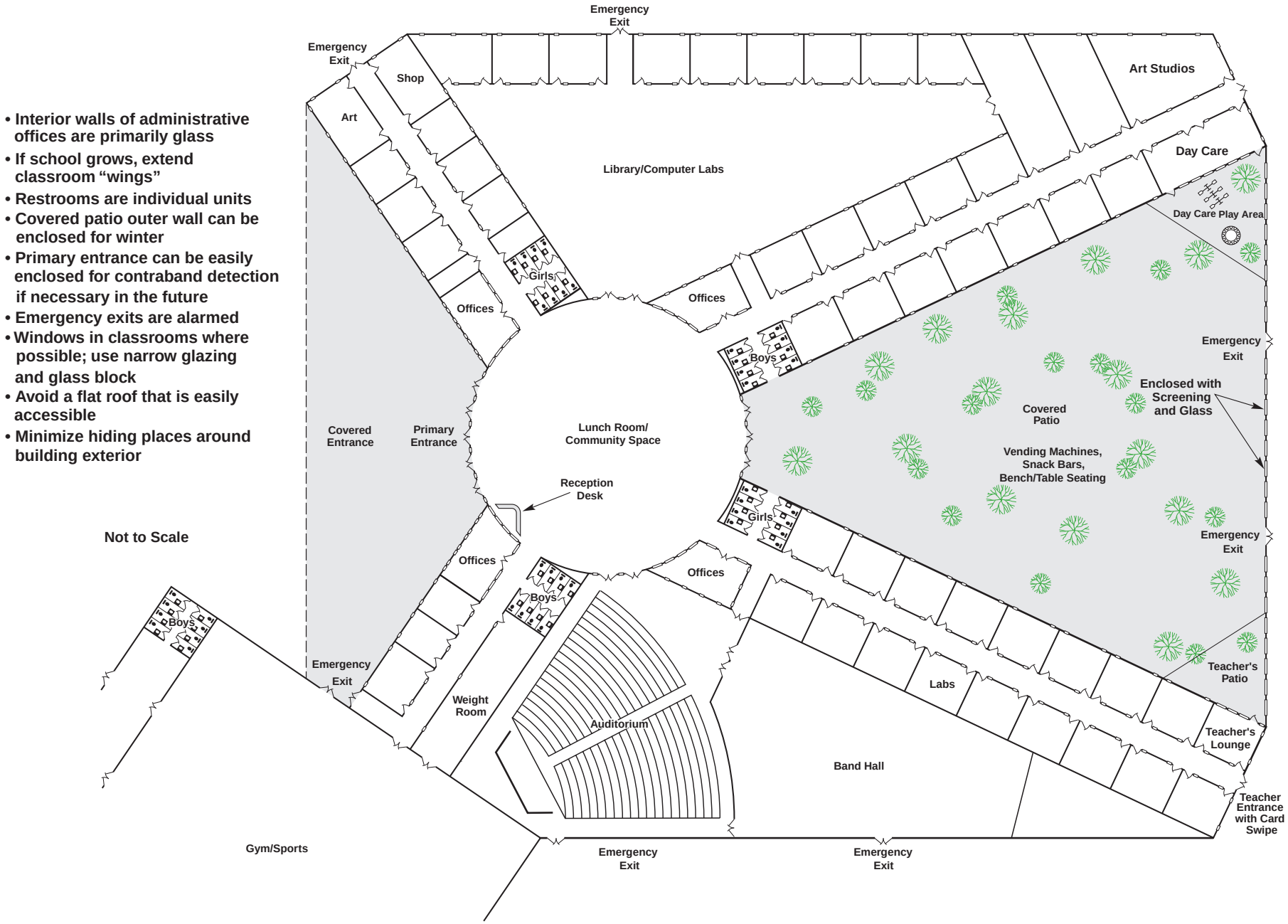


Exhibit 1.10. This drawing depicts a school design that incorporates some security-conscious features.

If a school is perceived as unsafe (i.e., it appears that no adult authority prevails on a campus), then "undesirables" will come in, and the school will actually become unsafe. This is an embodiment of the broken window theory: one broken window left unrepaired will encourage additional windows to be broken. Seemingly small incidents or issues such as litter on a school campus can provide the groundwork for (or even just the reputation of) a problem school. Issues of vandalism and theft can be almost as harmful to a school as actual violence because they can create a fertile environment for loss of control and community confidence.

Issues contributing to a school's overall order maintenance must therefore be taken seriously, not unlike any other public facility. Reducing theft, deterring vandalism and graffiti, keeping outsiders off campus, keeping the facility in good repair, improving poor lighting, maintaining attractive landscaping, and getting rid of trash are all important to school security (exhibit 1.11).

Technologies such as cameras, sensors, microdots (for identifying ownership), and antigraffiti sealers can contribute significantly in many (but not all) situations and are possible approaches to further support a school's order maintenance.

Too often school districts undervalue the ultimate importance of reliable and conscientious maintenance, janitorial, and groundskeeping staff. Their ultimate contribution to the order maintenance of a school can be enormous. Additionally, the janitorial staff needs to be selected with almost the same care as the teaching staff because they have great access to and knowledge of a school facility. Contracting out this work without complete background checks of all workers can lead to many problems in the long run.

Exhibit 1.11. Keeping a school well maintained and litter free is paramount in a school's order maintenance.

Chapter II Video Surveillance

A. Video cameras

1. Why video cameras?

The peace of mind of both students and faculty at a school can often be quickly enhanced by the installation of video cameras as part of a closed circuit television (CCTV) system. This change of attitude may result in even further-reaching effects on a campus than would be expected by the use of cameras alone. As mentioned in the introductory chapter of this guide, a sense of safety and authority will directly influence people's opinions and impressions, which will ultimately contribute to the overall order maintenance of a facility and how that facility is treated by occupants and outsiders.

To the school's security personnel who must handle day-to-day security issues, the best thing about cameras is the deterrence factor they introduce to outsiders who do not belong on campus and to students and employees who do. Information regarding security measures, such as cameras at the local school, will generally spread through a community. This type of reputation can make outsiders reconsider an unwelcome visit to the historically easy mark of the neighborhood—the school. It can be assumed that most kids are not going to step way out of bounds if they believe they will likely be caught, which is often possible through the appropriate application of cameras. In a school security system, the ideal goal should be to convince kids not to even attempt to do something that is unacceptable.

Addressing an incident after it occurs is good, but not as good as if it had never happened. Once a perpetrator is caught, there is a chain of events involving confrontation, denial, parental involvement, consequences, and perhaps even the involvement of law enforcement and the legal system. School administrators will be forced to spend a great deal of time on the matter, and all participants will find the process distasteful.

Another strength of cameras is the strong evidence they can preserve on tape. Even if law enforcement is not brought in regarding an incident, the recorded tape can be invaluable to a school administration. Many schools report that when students are brought into the school office after an incident and shown a tape of themselves in an illegal or unacceptable act—even if the tape might not have been of sufficient resolution and detail to use for prosecution purposes in a court of law—the student will usually admit to the incident.

The ultimate usability of a video recording is dependent on many variables. It is possible for a camera system to produce tapes on which individuals are unidentifiable or their actions are indiscernible. Be certain that a camera system provides the kind of information you need before you pay for it. These requirements should be clearly spelled out in the purchase agreement, along with a specified time period during which the school can adequately test it.

Video recordings are also beneficial for use with parents. Although nearly all parents want to believe their chil-

Exhibit 2.1. Examples of cameras and camera housings.

dren are innocent of wrongdoing, some parents will deny their child's guilt despite the credible testimony of others to the contrary. However, as many school administrators and teachers have discovered, parents quickly accept their child's role in an incident when shown a videotape of the incident. Most parents want to do the right thing, but hard evidence is often required for some to concede over a matter involving their own child.

From a cost standpoint, the use of CCTV in public areas on school grounds can free up manpower. If cameras are covering a large patio area where students congregate during breaks, adults who normally would be assigned to oversee that area can instead be made available to monitor other areas of concern.

Finally, the solid documentation that a video recording provides can be invaluable in situations involving liability claims. Although it is possible that this may occasionally work against a school, most schools welcome this concrete evidence so that testimony regarding an incident does not consist solely of hearsay.

2. Why NOT video cameras?

- CCTV systems are expensive. Installation can also be expensive, as well as logistically difficult.
- Choosing the correct camera equipment requires some technical knowledge (exhibit 2.2).
- A single camera can effectively view a smaller area than would be intuitively expected, hence many applications can require more cameras, equipment, and expense than was originally expected.
- Cameras can be stolen or vandalized.
- Ongoing maintenance and operational support are required.
- Some applications or areas do not warrant camera use.
- Some communities or individuals will challenge the legality of using cameras.
- Insiders with full knowledge of the installed video system's capabilities can possibly circumvent the system to their advantage.
- If it becomes well known where cameras are being used at a school, students may simply move their misbehaviors to a different part of campus.

3. Good applications versus poor applications

An effective use of cameras in schools is viewing the recorded tape after an incident has occurred. Examples of reasonable goals for a school video system are capturing scenes indicating who started a fight in the hallway, who is smoking marijuana in the parking lot, who stole all the blank computer disks out of the computer laboratory, or if a particular person did indeed try to run down someone with his or her truck in the school driveway. Less reasonable goals, or at least more difficult or manpower intensive, are trying to use camera scenes to stop a student fight in its early stages, prevent someone from bringing weapons into the facility, or catch a thief before he makes his escape.

A visible camera may not help if a school's goal is to identify a nighttime thief in the band hall or computer lab if the thief simply covered his or her face or disguised

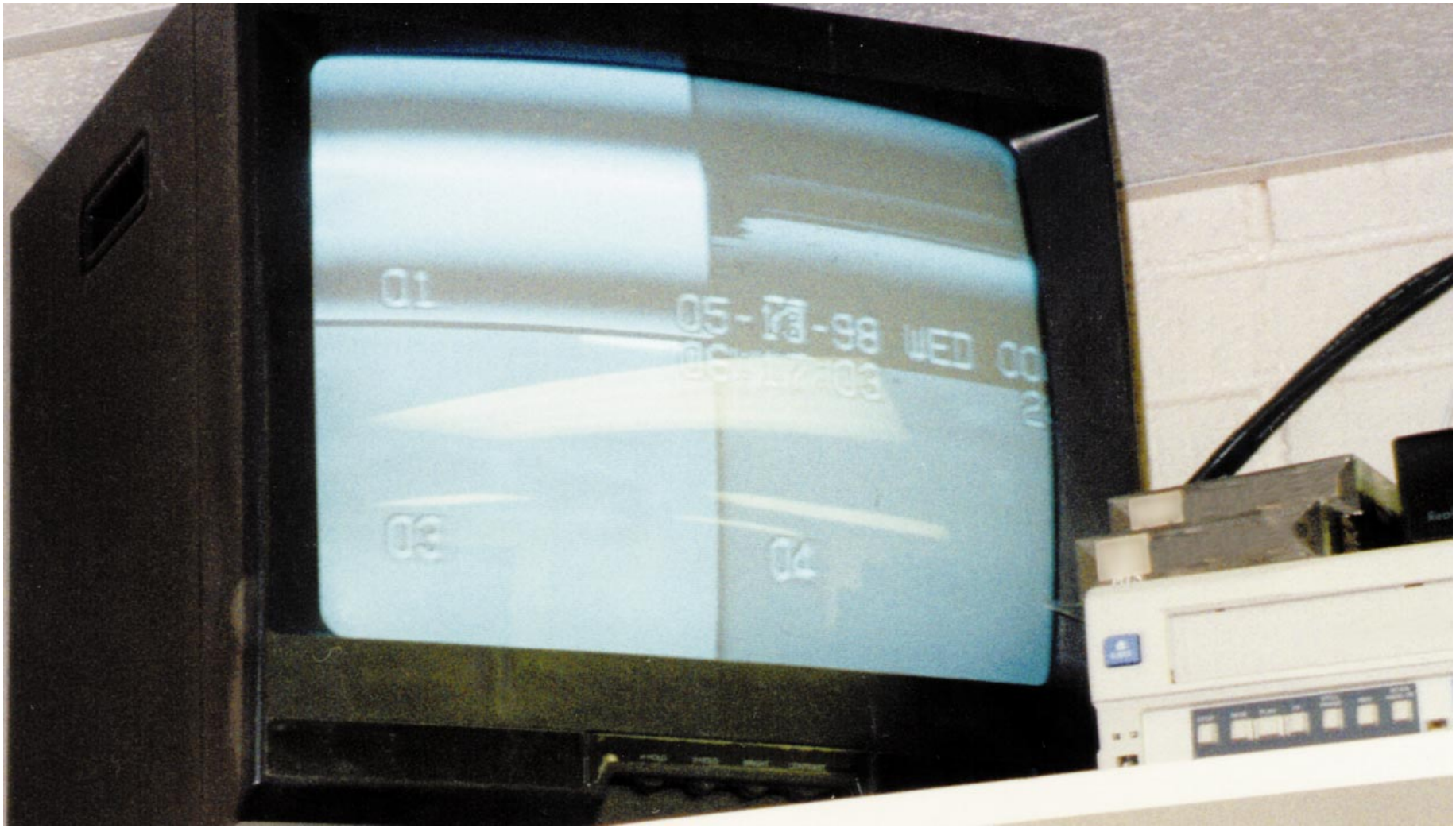


Exhibit 2.2. This photo shows the poor-quality images from a new camera system installed at a school. The installer had yet to debug the system 2 months after installation.

himself or herself. However, it may still add substantially to deterrence; a would-be thief may never be sure if there will be some type of immediate response to the video recording or exactly where all the cameras are located.

Depending upon each situation, video cameras can support security initiatives in the following applications:

- Parking lots and driveways.
- Cafeterias.
- Patio and entry areas.
- Hallways.
- Gymnasiums.
- Main administrative offices (exhibit 2.3).
- Band halls.
- School stores.
- Computer rooms.
- Science laboratories.
- Supply closets.

Schools may want to consider classroom installation of the cameras and recorder enclosures that are currently so popular for use on school buses. For buses, a camera is placed in the black box only when requested by a bus driver, thereby reducing the number of camera systems that must be purchased. Usually, the deterrence factor derived from students never knowing when a camera is actually present can discourage much of the misbehavior. (This is not to be confused with the use of a dummy camera, where a potential victim is under the illusion that he or she is being monitored and, therefore, help will be forthcoming in the event of an attack; this can create extensive liability concerns for a facility.)

In an application with a camera looking in an easterly or westerly direction, extreme glare may occur during sunrise or sunset. If this type of placement cannot be avoided, the camera should be mounted as high as possible and then angled downward to view below the horizon. If sunrise and/or sunset are not critical time periods for a particular application, then it may be acceptable to simply have an unusable picture during these times.

Similarly, vehicle headlights and other sources of glaring light, particularly during night operations, should be considered. A system that is designed with the potential problem sources recognized can be compensated for. After initial installation is complete, it is much more difficult to compensate for these problems. Oftentimes, funding is no longer available to make needed adjustments.

Viewing a scene such as a dark doorway that contains a significant shadow can be quite difficult (exhibit 2.4). Newer cameras with better electronics help compensate for these types of applications, but they are more expensive.

Seasonal problems should be anticipated and addressed before purchasing an exterior camera system. Conditions to be aware of are blowing snow, built-up ice on a camera housing, dust storms, trees that block the scene in summer, temperature extremes, or north sides of buildings with shadows that may affect scene assessment during winter months.

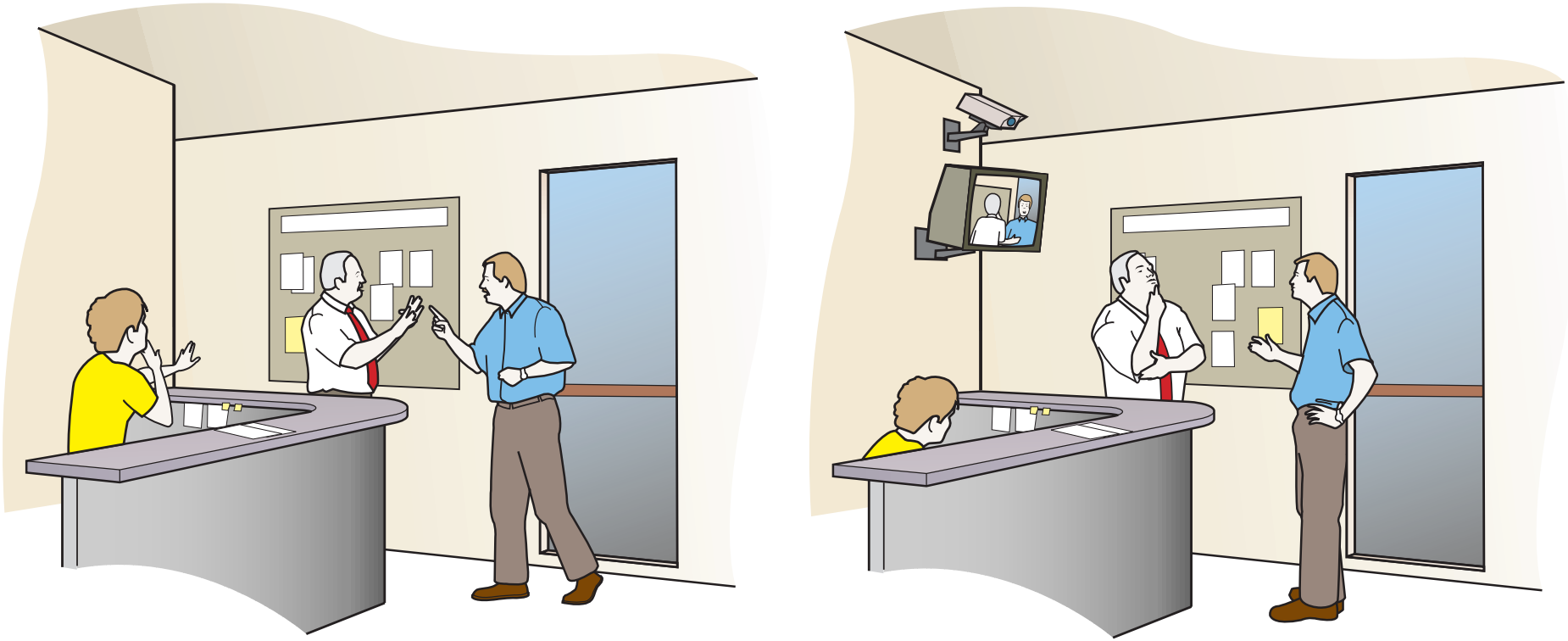


Exhibit 2.3. Occasionally, an irate parent may threaten a school employee, but this can be mitigated if the parent sees himself being recorded on a video monitor.

Exhibit 2.4. Dark spots caused by heavy shadows in a scene can be very difficult to assess with cameras.

4. To monitor or not to monitor

Each year, a great number of camera systems are bought in the United States with the objective of assigning a security person to constantly monitor the scenes from the video cameras in real time. The objective of such installations is that some sort of response may then be dispatched immediately and an undesirable incident prevented or stopped, basically using the live person watching the monitor as a detector. This is quite often an unrealistic approach to security, particularly in school applications.

Experiments were run at Sandia National Laboratories 20 years ago for the U.S. Department of Energy to test the effectiveness of an individual whose task was to sit in front of a video monitor(s) for several hours a day and watch for particular events. These studies demonstrated that such a task, even when assigned to a person who is dedicated and well-intentioned, will not support an effective security system. After only 20 minutes of watching and evaluating monitor screens, the attention of most individuals has degenerated to well below acceptable levels. Monitoring video screens is both boring and mesmerizing. There is no intellectually engaging stimuli, such as when watching a television program. This is particularly true if a staff member is asked to watch multiple monitors, with scenes of teenagers milling about in various hallways, in an attempt to watch for security incidents (exhibit 2.5).

A practical security application of real-time viewing of a video monitor might be the intent to actively allow or disallow individuals to enter a particular locked door. In this case, the security person at or near the video monitors receives an alarm or other announcement that a person desires entry into that facility or area. The security person would then focus his or her attention directly on the screen and make a decision (according to procedures) as to whether to release the remote lock on a door to allow the person access.

Most schools have a security staff, whether it be an assistant principal assigned security as one of his or her duties, a few security aides equipped with two-way radios, or an impressive number of sworn police officers. Few schools, however, find themselves with surplus security-staff time. Because of the ineffectiveness of people monitoring video scenes in real time, it would seem to be a very poor use of school security staff. One possible exception is when a certain incident is expected at a school during a finite time period. For example, if cars in a parking lot are frequently broken into during the noon hour, security staff may want to actively monitor their cameras' outputs during this period so that they may immediately assess an incident in progress and apprehend the suspect. This would be particularly appropriate if the suspect is not known and not a member of the school.

The use of cameras and a real-time display unit without the benefit of a recorder is not recommended. It is true that a video camera and monitor alone are much cheaper than a complete video system with recording and multiplexing capabilities. However, the hard evidence made available in the form of a video recording can more than make up for the cost of a recording system. Ease of prosecution and the likely prevention of future incidents by this individual are additional benefits.

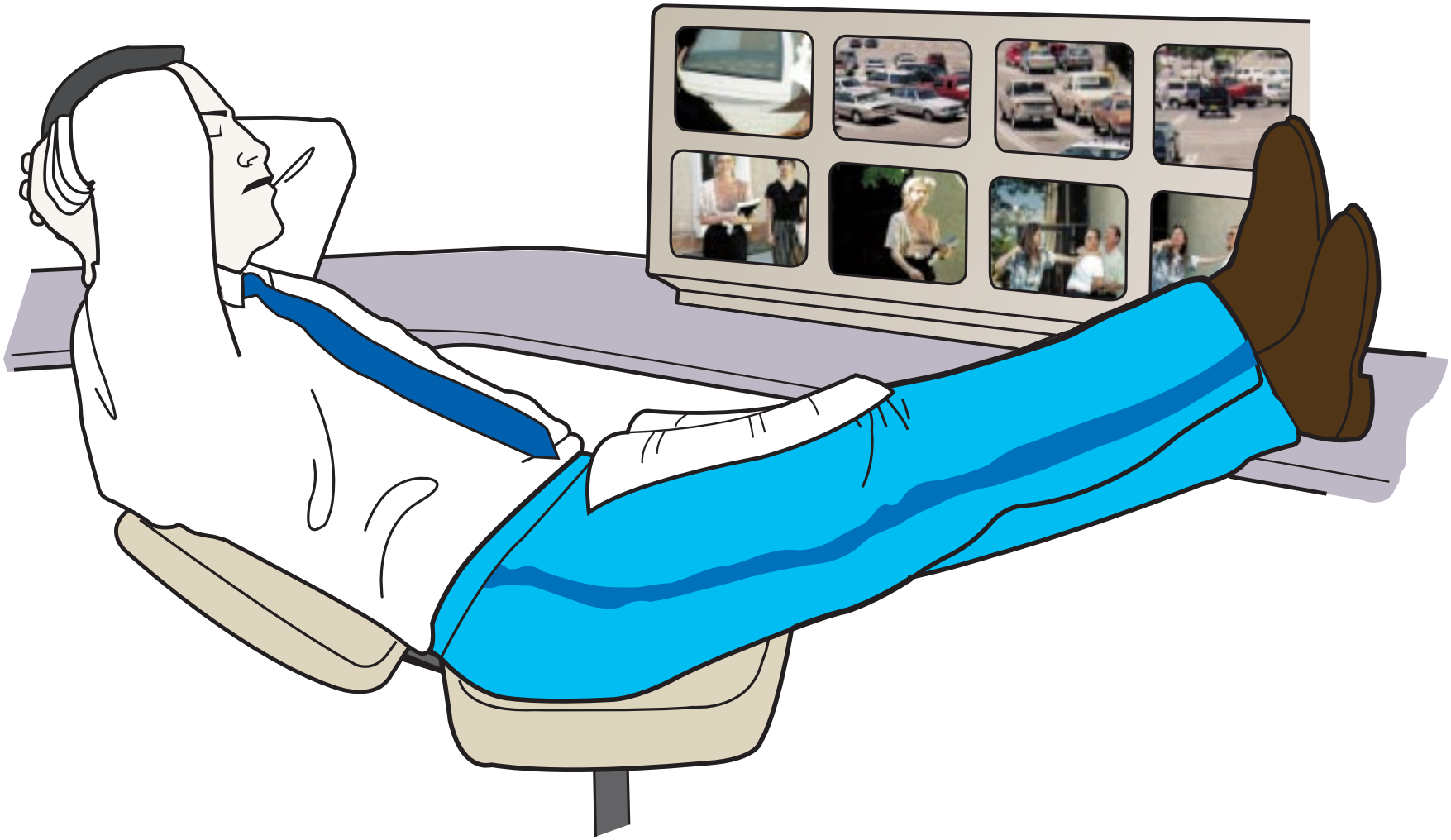


Exhibit 2.5. Monitoring video output is a boring task and usually nonproductive in most security applications, even for the motivated employee.

5. Color versus black-and-white cameras

In a high-security application, when an alarm has been generated signaling a presence in an off-limits area, it is likely to be sufficient to be able to assess the alarm condition with a black-and-white camera. The objective here is merely to determine that it is a person intruding (any person) and that a response should be prepared or dispatched.

In a school application, the security objective of recording video scenes would generally be to determine who the perpetrator of an incident was. In this type of after-the-fact assessment, it is most important to identify, not just detect, the intruder. Because of this, color cameras are probably more helpful for most school applications than black-and-white cameras. Color recordings will contain much more information about the scene that was viewed, i.e., the boy who broke the window had red hair, a dark yellow jacket, and drove away in a light blue car. This can be critical for school applications; the school principal can match the characteristics of the recorded suspect with those of students or outsiders known to frequent the area. Quite often, when a suspected student is brought in and shown a recording of himself or herself in an incident, he or she will admit to a role in it, even though there may not have been quite enough detail on tape for a positive identification.

Color cameras usually have lower resolution than black-and-white cameras. However, for the school application, the ability to recognize the color of clothing, color of vehicle, and so forth is often more important than a more detailed image. The amount of information on a video recording that is required to prosecute a suspect in a court of law may be much greater in many instances than what a school video system will normally collect.

The cost of color cameras is slowly approaching the cost of black-and-white cameras. Currently, the cost of a color camera as compared to an equivalent black-and-white camera is anywhere from 30 percent to 70 percent greater. Most school applications will find the higher priced color cameras necessary for their goals. An exception to this would be a camera applied in a small interior room or area where any potential perpetrators will be close enough so that their faces will be easily identifiable in black and white.

When using either black-and-white or color cameras under low light level conditions (such as at night with artificial lighting) it is necessary to evaluate the effectiveness of the existing lighting. Generally, security applications of cameras require higher light levels and more evenly distributed lighting than is found in parking lots with typical safety lighting. Also, if school officials plan to use their cameras for nighttime applications, color cameras will require a higher lighting level than black and white cameras. (See the section on lighting requirements and nighttime applications.)

6. Fixed versus pan-tilt-zoom cameras

Two types of camera configurations are available on the market: the fixed camera and the pan-tilt-zoom camera. Fixed cameras are mounted in a stationary position (although what the camera is mounted on may actually move, such as on a police vehicle). These cameras will view the same scene until physically relocated. The scene is typically recorded and, less often, the scene is also viewed simultaneously on a monitor by security personnel.

Pan-tilt-zoom cameras can operate in either of two modes. The mode for which these cameras are most useful allows the scene that is viewed to be controlled by an operator sitting at a video monitor. This operator can control the direction and angle of the camera as necessary. These cameras typically have a zoom option that will allow the operator to focus on parts of a scene, such as zooming in on a suspected perpetrator. The second mode for pan-tilt-zoom cameras is an automatic mode, in which the camera automatically scans back and forth over a certain portion of its range. Normally a pan-tilt-zoom camera should be protected and shielded from view by an opaque enclosure (domes are quite common) so that it is difficult for a would-be perpetrator to tell where the camera is actually aimed.

Most applications in schools are better served by fixed cameras. One consideration is that the pan-tilt-zoom camera can cost around three to five times as much as an equal quality fixed camera. More important, though, is the fact that pan-tilt-zoom cameras, when run by an operator, consume the time of a security staff member. When run in automatic mode, the chance of the pan-tilt-zoom camera looking (and recording) in the direction where an incident is occurring is much less likely than the chance that it will be looking in the wrong direction (exhibit 2.6). Pan-tilt-zoom cameras also introduce a mechanical component to the system that will require more regular maintenance (e.g., oiling gears, replacing motors, and so forth) and that will be one of the more likely fail points.

Pan-tilt-zoom cameras may be employed during a fixed portion of the day, such as the lunch period, if an operator is available to watch and track suspects with this camera. Gateway High School in Denver, Colorado, has a dozen fixed cameras located throughout the campus but also successfully uses one pan-tilt-zoom camera overseeing the parking lot that allows an operator to watch suspected perpetrators before and after classes. Gateway's goal is to record a suspected individual while he or she is involved in a regularly occurring incident of which the school is already quite aware.

With these considerations, it would usually be more cost-effective and more reliable to capture incidents using multiple fixed cameras looking in different areas from a single point than to use a single pan-tilt-zoom camera. (This does not take into account installation costs.)

7. Hardwired versus wireless systems

Traditionally, camera systems have cabling that runs directly between the camera and the recording mechanism (or viewing monitor). These hardwired runs are usually recommended by manufacturers to not exceed 500–1,000 feet, using RG–59 coaxial cable. Signal equalizers/amplifiers will be required to compensate for signal loss if distances become much greater than 1,000 feet. See exhibit 2.7 for typical transmitting distances.

For exterior applications, cabling for camera systems should be placed within a watertight conduit. Underground cabling should be buried below the frostline or a minimum of 24 inches deep. Direct buried cables (without conduit) are subject to damage by rodents (if no rodent shield is provided), accidental digging, and intentional tampering. Above-ground cabling that is not in a conduit is very susceptible to tampering, as well as environmental degradation. With coaxial cable runs, ground loops (in video applications, this is a current flowing along

Exhibit 2.6. A pan-tilt-zoom camera that is set to automatically pan an area may completely miss capturing incidents of concern.

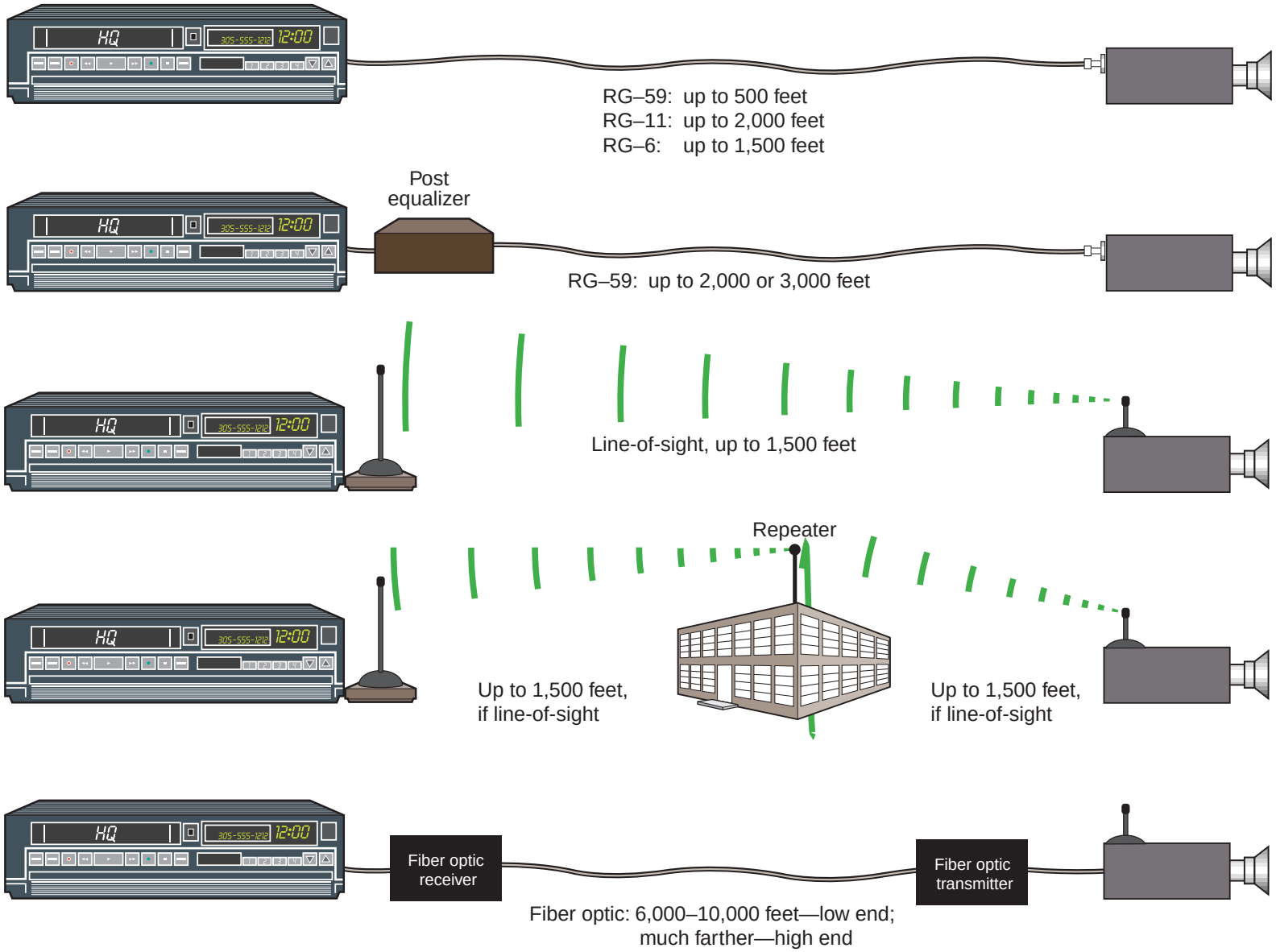


Exhibit 2.7. This diagram illustrates typical maximum transmitting distances for hardwired and wireless camera systems. (Note: Some cameras have "pre-equalization" that will allow signals to go 1,000 feet farther than typical RG–59 signals.)

the shield of the coaxial cable due to a voltage difference in the ground between the ends of the cable) and interference from radio frequencies (RF) or other signals must be considered. Coaxial cables should not be run next to, or parallel with, power lines over long distances. Equipment, such as hum transformers and electronic video clamps, is available in instances where interference is a problem.

With exterior coaxial cable runs, close lightning strikes can induce voltage surges on the cable that can damage equipment on both ends. To protect equipment, surge protectors are installed at both ends of the cable run.

Fiber optic cabling is an excellent alternative to coaxial cable. With fiber optics, there are no concerns with noise, RF interference, ground loops, or voltage surges. Fiber optic systems require a transmitter at the camera end and a receiver at the monitoring end. Fiber optic systems are more costly than coaxial cable systems for short runs but become more cost effective with longer cable runs (greater than 3,000 feet). Installation of fiber optics is also more expensive, requiring trained and experienced installers and specialized tools for handling and connecting.

For interior applications, cabling for hardwired camera systems should be placed within a metal conduit if it is exposed or accessible by building occupants, including maintenance staff. A good example of this is cabling run above loose/replaceable ceiling tiles.

Short-distance, low-power RF wireless camera systems for video signal transmission are becoming more popular. (Wiring is still required for power.) A transmitter is required at the camera, as well as a receiver at the recording end. This will add an estimated $1,000 or more to the price of the system for each distinct camera location (multiple cameras can be at one location, as in exhibit 2.8). In many cases, however, wireless may be cheaper (and certainly easier) than running cabling.

Acceptable distances between a transmitter and receiver may range up to about 1,500 feet if the camera transmitter is in direct line-of-sight of the receiver. If equipment is located such that data transmissions must go through walls, fences, and so forth, the detail of the transmission can quickly degrade if the transmitter/receiver distance is already close to the manufacturer's recommended maximum distance. Installation distances to be implemented for camera transmissions should be much less than manufacturer recommendations if the transmitter and receiver are not within each other's line of sight.

The advantage of wireless camera systems is, of course, that cabling does not have to be run underground, through the air, or behind walls and ceilings. Therefore, the chance of tampering is much less. However, wireless applications where distances are close to manufacturer limitations may experience interference from very unusual sources, e.g., a nearby parked truck. Previous installation experience is usually required to set up such a system, due to the different antennas available that can perform differently in unique setups.

Short-distance, low-power RF transmission systems, such as a school's wireless camera system, usually do not require licensing by the Federal Communications Commission (FCC). Higher power systems will require an FCC license.

Exhibit 2.8. These bullet-resistant cameras on the light pole of a school parking lot were installed using wireless technology for data transmission. This configuration, which required line of sight between the transmitter and receiver, greatly reduced the expense and difficulty in running protected cabling back to the recording equipment. Note the protective shielding for the power cables that serve each camera.

8. A more technical discussion of formats, resolution, pixels, lenses, and field of view

A basic familiarity with camera terminology is probably adequate for most school administrators who plan to go out on bid for a CCTV system. However, for the benefit of those who might be responsible for choosing or upgrading camera equipment, the following discussion presents these technical specifications in more depth.

Formats. Camera format relates to the size of the camera imaging device. Most solid-state cameras used in security applications today are $^1/_2$-inch or $^1/_3$-inch format. There are some $^2/_3$-inch cameras still in use, and some $^1/_4$-inch format cameras are beginning to appear on the market. The trend has been to make camera formats smaller as picture element densities have increased, giving the manufacturer more imaging devices per production run, reducing costs, and allowing for smaller cameras.

Resolution. Resolution is the ability to resolve or see small details in an image. Resolution for CCTV cameras (as well as for TV monitors and recorders) is usually specified in terms of horizontal lines of resolution. Horizontal lines of resolution relates to the number of independently resolvable elements (small details) in three-fourths of the picture width. CCTV cameras range from 200 to more than 1,000 lines of horizontal resolution. Higher resolution cameras generally cost more than lower resolution cameras. For a typical color security camera system (system includes camera, cabling, recorder, and TV monitor) that uses a standard National Television Systems Committee (NTSC) color video signal format, 300 to 400 lines of horizontal resolution are common. Black-and-white systems for tighter security applications typically range from 500 to 700 lines of resolution. Cameras with more than 800 lines of resolution are commonly used in broadcast TV, medical, or industrial applications.

Pixels. Active picture elements, sometimes referred to as pixels, is a term used specifically with cameras and is directly related to horizontal lines of resolution. Active picture elements are the actual number of light-sensitive elements that are within the camera imaging device. Active picture elements are expressed with a horizontal number (the number of elements horizontally across the imager device) and a vertical number (the number of elements vertically on the imager). A camera specified with 768H by 494V picture elements has 494 rows of picture elements vertically, with each row having 768 elements horizontally. For black-and-white cameras, horizontal lines of resolution relate to picture elements by a three-fourths factor (by definition of horizontal lines of resolution) so a black-and-white camera with 768 active picture elements will have 576 horizontal lines of resolution. This would hold true for color cameras as well, except that the NTSC format limits signal bandwidth which reduces resolution.

Lines of resolution, camera format, and lens focal length (discussed later) are the camera-specific part of what determines if a camera scene will be useful for a particular application. Other items to consider include lighting, shadowing, camera aiming, and camera sensitivity. Before selecting a camera and lens combination for an application, one must determine what is desired to be seen in the image. Just being able to see a person in a specific area, such as a parking lot, will require one set of minimum criteria for camera and lens selection. Being able to identify a person by facial features (if the person faces the camera) will require a different set

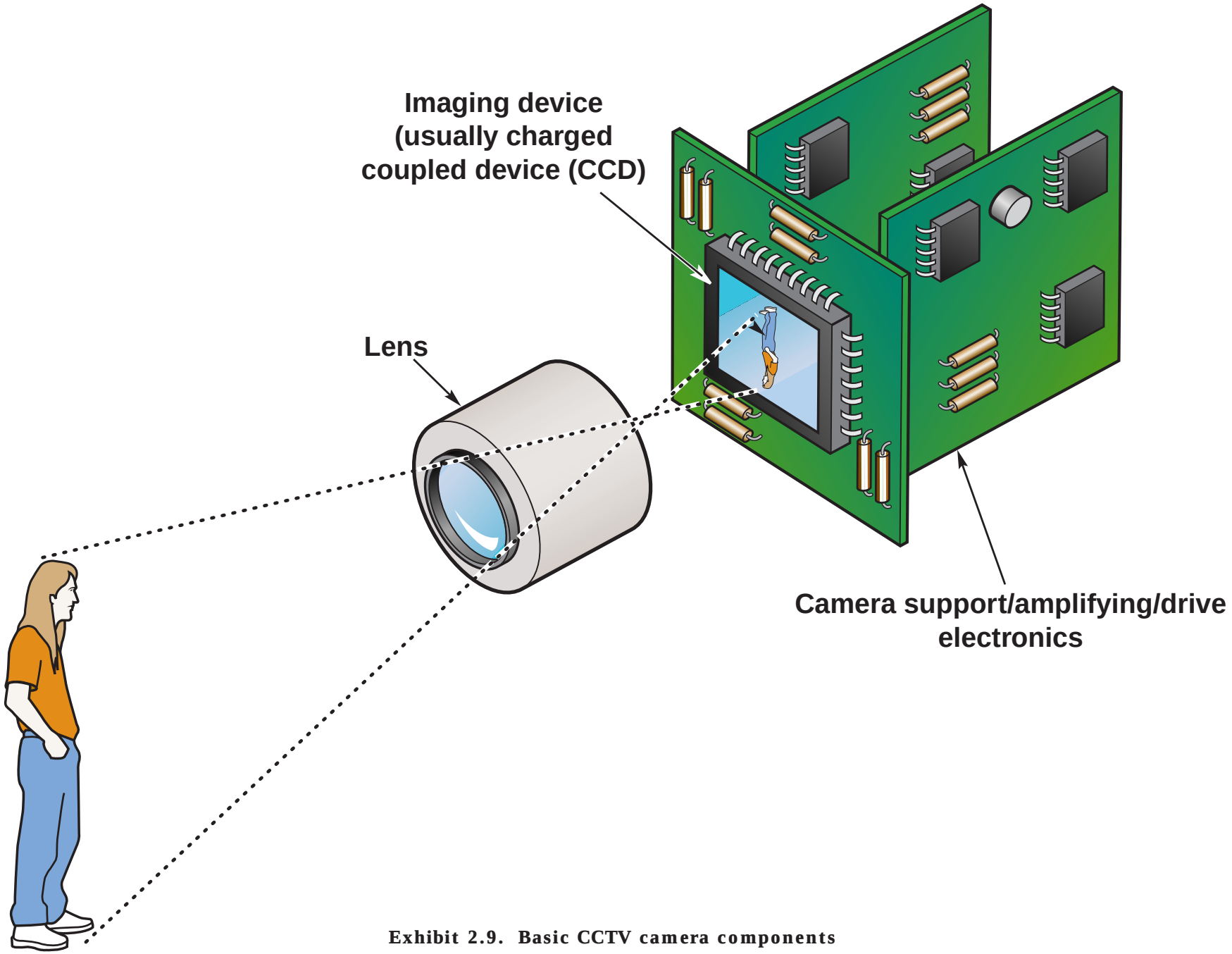


Exhibit 2.9. Basic CCTV camera components

of criteria. For identification purposes, a person must be much larger in a scene than for the purpose of just determining if a human is present.

Because a camera scene is observed on the TV monitor, the entire CCTV system resolution must be considered. This includes the camera and lens combination, the camera signal transmission equipment (such as coaxial cable and amplifiers), the TV monitor, and the recorder. All components of the system must have adequate resolution for the application desired.

For observation of a camera scene to determine only if a human is in the scene (or to be able to distinguish between a person and an animal), a minimum criteria of 6 horizontal TV lines across a 1-foot-wide object within the scene is used. (In terms of active picture elements, this means that a 1-foot-wide object would cover 8 horizontal active picture elements for each row of picture elements for the height of the object on the camera imager.) For identification of a person by facial features, 16 horizontal lines (21 pixels) of resolution subtending a 1-foot-wide object is needed.

The lens focal length (discussed in the next section), camera format, and how far an object is from the camera will determine how large an object is within the scene, as well as how many active picture elements the object covers on the camera imaging device. Higher resolution cameras (for example, 576 horizontal lines or higher) can be used to distinguish objects farther away (smaller in the scene) than a lower resolution camera (approximately 250 horizontal lines) allows. In other words, an object can be smaller in the scene for higher resolution cameras and still meet the minimum horizontal resolution criteria. The significance of this is that fewer higher resolution cameras will be needed than low-resolution cameras in some interior and many exterior applications.

Lenses. A camera lens focuses light reflected from objects within a scene onto the imaging device of the camera. The imaging device converts light to an electrical signal. Lens focal length and aperture are two important parameters to consider.

Lens focal length describes the relative magnification of the lens. The camera field of view (defined below) will be dependent on the lens focal length, along with the camera imager format size. Similar to the camera imager format, there is a format size for lenses. For most cases, the lens format size should be matched to the camera imager format size. Mismatched format sizes can result in the focused image being too large or too small for the camera imaging device. Different camera and lens formats can be used satisfactorily in a few instances.

Except for the most uncommon sizes, there usually is not a large price difference between various lens sizes. The most common sizes are 4.8mm, 5.6mm, 8mm, 12mm, 16mm, 25mm, and 35mm. A 35mm lens has the longest range with the narrowest field of view. The 4.8mm lens can see much shorter distances, but it will have a much wider field of view. Most lens sizes can be used in exterior applications, depending on the view desired. Shorter focal length lenses, such as 4.8mm or 5.6mm, are typical for interior applications, due to the shorter distances involved.

The important thing to consider is that the camera field of view depends on the focal length and format size. Camera field of view is expressed in horizontal and vertical angular fields of view. Most camera manufacturers or manufacturers' representatives who sell lenses with their cameras can provide charts that list the angular fields of view for common lens sizes. Exhibit 2.10 shows the difference between two different lens focal lengths.

The lens aperture, or speed of a lens, is a relative measure of the ability of the lens to gather light. Aperture is expressed as the F-number. The F-number is the ratio of lens focal length to its clear aperture. Clear aperture is the diameter of the inside of the lens where light passes through when the lens iris is fully open. A lens that is designated as an F/2 will have a clear aperture size that is one-half its focal length, meaning that a 16mm focal length lens will have a clear aperture of 8mm. The lower the F-number of a lens, the more light the lens can gather. This becomes important when operating a camera at low light levels, such as at night with artificial lighting. Most security camera lenses today have F-numbers of 1.8 to 1.4. These are usually adequate for night applications given that the minimum light levels for CCTV are provided.

Not all lenses are the same, however. Two different lenses with the same F-number can have different light-gathering capabilities. This is particularly true when it comes to fixed focal length lenses versus variable focal length (zoom) lenses. Zoom lenses have more glass elements than fixed focal length lenses. Because of the additional glass elements, an F/1.8 zoom lens will not be able to pass as much light as an F/1.8 fixed lens with fewer glass elements. An amount of light transmission is lost in each glass element. This is important to consider during night operation under artificial lighting. A zoom lens will require higher lighting levels than a fixed focal length lens if an equivalent picture quality is desired.

Most lenses for security cameras will have an adjustable iris to control the amount of light that is received at the camera imager. The iris is either manually adjustable or electronically controlled. The electronic iris (or auto-iris) monitors the camera video signal output and will open the iris for decreasing light levels and close it for increasing light levels. This keeps the video level (brightness and contrast) fairly constant under varying lighting conditions. In the case of a manual iris lens, the user or installer adjusts the iris opening for the proper video signal level for the expected operational lighting level. If light levels change, an adjustment to the iris will be required in order to maintain a proper video signal level. Manual iris lenses are used mostly in interior applications where no outside light comes in and the light levels remain constant. For all exterior and many interior applications, an auto-iris lens will be necessary.

A relatively new feature in many cameras is the electronic shutter. The electronic shutter is part of the imaging device and can perform close to the same function as an electronic iris. It controls the amount of light that the light-sensitive elements within the camera imager receives. Electronic shutters have limitations, however. They may not have as much range as auto-iris lenses. This is an important consideration for exterior applications. If light control is totally dependent on a shutter (a manual iris lens is used instead of an auto-iris) in an exterior application, the shutter may not be able to reduce light enough on bright, sunny days,

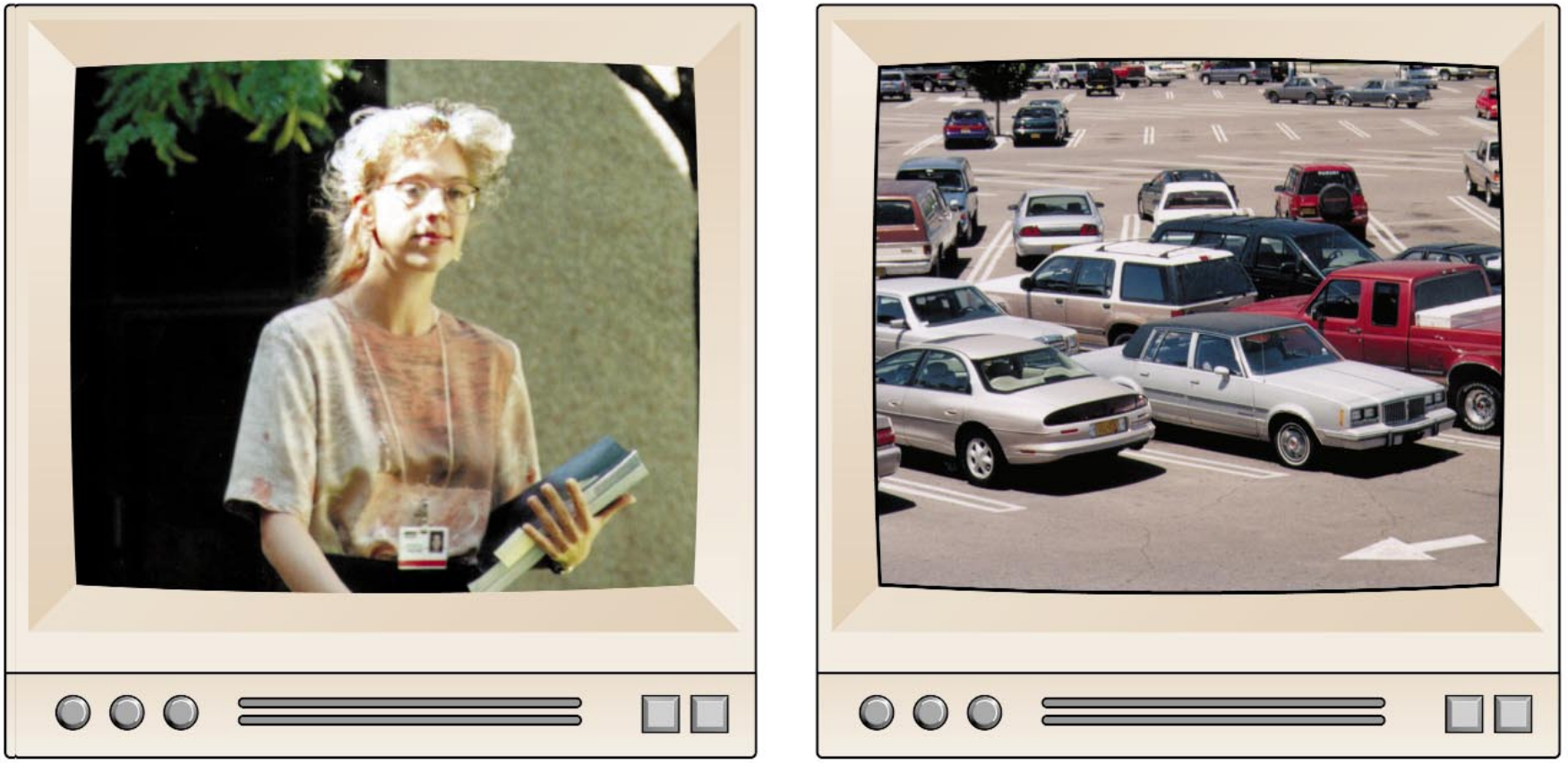


Exhibit 2.10. The left-hand image demonstrates a camera lens focal length of 4.8mm. The right-hand image uses a focal length of 16mm.

resulting in portions of the picture washing out. If the manual iris lens is partially closed to compensate for bright sunshine, low-light conditions may produce a dark, noisy picture. Many shuttered cameras intended for exterior use will also come with an auto-iris lens.

Field of view. Field of view (FOV) relates to the size of the area that a camera will see at a specific distance from the camera. The field of view is dependent on lens focal length and camera format size.

The FOV width and height can be calculated using the following formulas:

$$\text{FOV Width} = \frac{\text{Format (horizontal in mm)} \times \text{Distance in feet from camera}}{\text{Focal length}}$$

$$\text{FOV Height} = 0.75 \times \text{FOV width}$$

Manipulating the FOV formula allows a calculation of the distance in feet from the camera for a required FOV width. The formula becomes:

$$\text{Distance (in feet from camera)} = \frac{\text{FOV width} \times \text{Focal length}}{\text{Format (horizontal in mm)}}$$

Before the FOV for a camera is selected, the minimum desired resolution for an intruder or object to be viewed must be determined (i.e., whether it is desired to identify a person or to just determine if a person is within the scene). This will limit the maximum FOV width and is referred to as the resolution-limited FOV (exhibit 2.11). The resolution-limited FOV width can be determined by using camera resolution in horizontal lines per foot and the number of lines of resolution per foot required to identify an intruder. The following formula is used to calculate the resolution-limited FOV width:

$$\text{Resolution-limited FOV width} = \frac{\text{Camera resolution}}{\text{Number of lines of resolution}}$$

A resolution of 16 lines per foot is considered acceptable for identifying most people. If a camera with 350 horizontal lines of resolution is utilized, the resolution-limited FOV width for a resolution of 16 lines per foot can be calculated as follows:

$$\text{Resolution-limited FOV width} = \frac{350}{16} = 22'$$

The following table presents the horizontal camera format sizes of the imager for various size imagers: Example: Calculate the maximum distance from a 350-line, horizontal resolution, 1/2-inch format camera with a 75mm lens to the resolution-limited FOV width at 16 lines per foot resolution.

Camera imager format size	1/4-inch	1/3-inch	1/2-inch	2/3-inch	1-inch
Horizontal format	3.0mm	4.9mm	6.4mm	8.8mm	12.8mm

$$\text{Distance} = \frac{22 \times 75}{6.4} = 258'$$

Exhibit 2.11 illustrates that there is camera coverage beyond the resolution-limited area but the resolution will decrease as the distance from the camera increases. People may be seen but not identified beyond the resolution-limited FOV area. The figure also demonstrates that, as people walk toward the camera and into the blind area, they disappear from view starting with their feet.

Another method of calculating the field of view is to use a lens selection wheel. These are mechanical computing

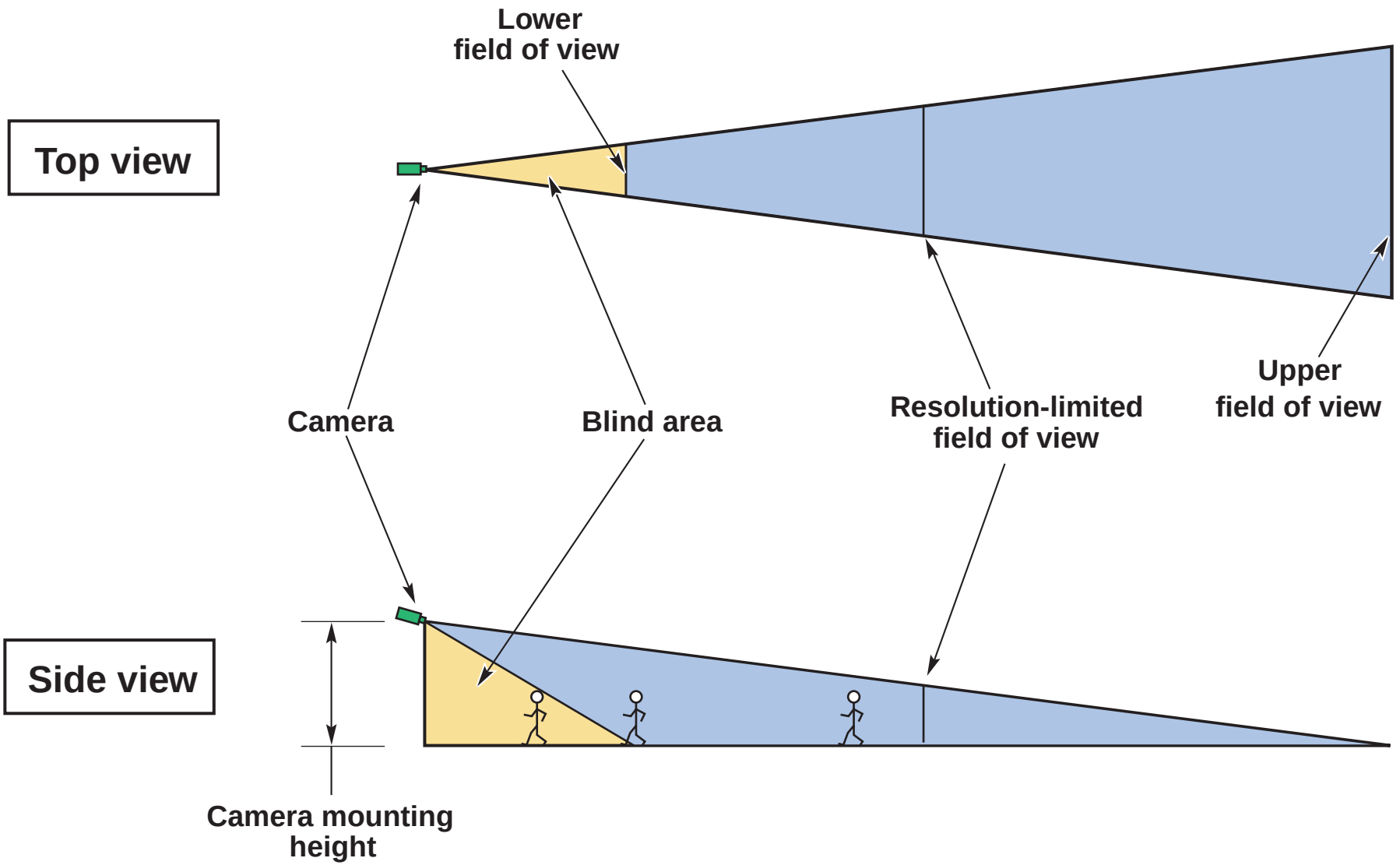


Exhibit 2.11. Field of View Camera Coverage

wheels that are available from many lens manufacturers and CCTV manufacturers. They will give a good approximation of FOV parameters.

A viewfinder can also be used to determine the field of view of a lens. This is a specially designed lens through which one can view the scene of interest. The scene is masked through the lens in such a way as to represent the picture that will be seen on the monitor. The scene desired can be dialed up on the viewfinder and the focal length of the lens required for the particular imager format size of the camera read from the side of the viewfinder. A viewfinder only determines a lens focal length value; other parameters must still be calculated.

Some lens manufacturers have developed tables for determining the field of view. The format size and focal length of the camera is cross-referenced to the column of the desired distance, and the width/height of the field of view is read from that column.

In summary, whether a camera scene is useful depends on whether objects can be distinguished in the scene. Camera resolution, camera format size, lens focal length, as well as lighting, shadowing, camera aiming, and camera sensitivity all play a role in being able to distinguish objects. Resolution and performance of other components such as TV monitors, recorders, and signal transmission equipment must be considered also. Cameras are specified with the number of horizontal lines of resolution and active picture elements. Most security cameras available today range from 300 to 700 horizontal lines of resolution. Black-and-white security cameras commonly have a horizontal resolution of 500 to 600 lines, while color cameras for security applications have 300 to 400 lines. In many exterior applications and some interior applications, a greater number of low-resolution (200–300 lines) cameras may be necessary in order to distinguish objects than would be necessary using higher resolution (500–600 lines) cameras.

9. Camera housings

One of the first considerations in selecting a camera housing is the environment. Is the camera to be installed outdoors or indoors? For indoor housings, the overall conditions where the camera is to be installed must be considered. Is the camera to be installed in a classroom, pool area, gymnasium, hallway, lobby area, or inside a school bus? A camera housing design can either help or hinder the installation and maintenance of a camera. In the outdoors, a watertight housing is desired; in some areas a heater may be required. Good ventilation is required in warmer climates. Domed enclosures are a special version of housings that can be used to conceal the position of the camera(s) via the use of viewing windows and various liners. The dome housing may also offer a more attractive look that can be designed to blend into its environment.

When installing housings in areas that drop below 30°F, the housing should have a heater. This is not so much to keep the camera warm as it is to protect the lens and to keep the viewplate free from condensation. Many auto-iris and zoom lenses can begin to experience mechanical problems at temperatures close to and below freezing. For this reason, the housing heater should be located toward the front of the housing, preferably in a U-shape or circle around the lens area. This will keep the lens warm and the front faceplate clear. The camera itself will provide ample heat (under most conditions) to keep it operational. Check the specifications listing for the camera's operating temperatures. In extremely cold environments, it may be

necessary to purchase a housing that is also insulated. Extremely cold environments would be any location where temperatures drop to less than -30°F.

A sunshield may be required in some locations. A sunshield can provide artificial shade and serve as a glare screen. A sunshield can lower the internal temperature of a housing by 10–15°F and can reduce the effects of sunrise/sunset glare. Dome housings, because of their overall design, do not usually have a sunshield option.

In warmer climates, housing ventilation may be required. Many housings or domes have an optional fan attachment and air vents. Filters over the vents will need to be cleaned or replaced on a regular basis, thus adding to maintenance requirements. Sealed housings with fans for heat dissipation or condensation control can be used, but are usually more expensive.

Humidity can do the most damage to cameras and other electronic equipment. If the camera is to be installed in an obviously high-humidity area, a pressurized environmental housing may be required. These are purged and pressurized with dry nitrogen. The sealed pressurized housing ensures that changing outside pressures will not force any dirt, humidity, and/or oxygen into the tube. Cabling for these units is installed through the back via a specialized plug.

Corrosion caused by salt can be a major problem in areas of the country with high humidity that are near an ocean (such as Florida). In pool areas, chlorine is a problem. These different types of corrosives can reduce the life expectancy of a camera or lens dramatically. Therefore, if an environment is considered corrosive, only those housings or domes that are considered environmentally sealed should be used.

A camera's vulnerability to vandalism must be taken into consideration (exhibit 2.12). A housing or dome that can accommodate a lock may be required. To prevent tampering, the housing should be made of steel, although fairly tough plastic housings are available. Such tamper-proof housings or domes are often made of 10-gauge (or higher) steel.

Some situations call for bullet-resistant housings. These units are usually constructed of 12-gauge stainless steel. The front glass will be constructed of a ¼-inch or thicker Lexan-type material. Two squares of ¼-inch plate glass sandwiched around a ¼-inch square of Lexan can probably prevent scratching of the surface due to washing, wind, and dust.

When choosing a proper housing or dome, it is important to consider the actual dimensions of the unit. Refer to the camera and lens specification sheets to determine the size of the housing. Leave enough room for cable connectors. The objective is to keep the unit small but allow room for everything to fit and to be accessible. Ideally, the selected housing will allow the camera to be focused and the parameters adjusted while the camera is mounted inside the housing. This depends on the design of the housing. Some housings have a hinged cover, opening from the top, that allows for easy focusing and adjustment. If mounted inside near the ceiling, this type of housing may not be feasible. Some housings allow the cover to slide off the base for easy adjustment of the camera parameters.

The prices of camera housings vary considerably. When going out on bid, be certain that your requirements document includes the features you will need.

Exhibit 2.12. A visible camera overseeing a known trouble area can quickly dissipate a crowd, but be certain that you have provided a vandal-resistant or even bullet-resistant housing for the camera.

10. Placement and mounting

To avoid the effects of blooming, streaking, and glare, all of which can wash out the video image, exterior cameras should be mounted below the nighttime lighting sources and aimed downward to shun direct sunlight, especially that occurring during sunrise and sunset. This may require a minimum mounting height of 18–20 feet. An even higher mounting height will help prevent vandalism of the camera. Consider the height required if a truck can be parked directly beneath the camera, where a perpetrator could stand on the truck's cab to reach the camera. Cameras should always be mounted on solid surfaces to prevent wind movement and vibration. Wooden poles can twist with high winds over a period of time and cause the camera view to change. Under these conditions, the camera may periodically require direction alignment.

In the interior environment, cameras cannot be mounted higher than the ceiling so it may be easier for an intruder out-of-view of the cameras to vandalize or tamper with them. This situation can be helped if the scene viewed by two cameras includes the other camera, such as cameras mounted at each end of a hallway or room and aimed to include a view of the other.

Cabling to the cameras must be protected from vandalism and tampering. In interior installations, wires can be hidden from view and therefore protected by routing them through the ceiling and/or walls. However, the small amount of wiring that may run from the camera to the wall or ceiling must be in a conduit. Also be aware that employees with access to the ceiling could tamper with your camera wiring.

For exterior camera installations, the video and power cabling to the cameras should be installed in a conduit. For underground runs, special cabling for direct burial should be used if the cable is not installed in a conduit. The cable running up poles or buildings to the cameras must be in a conduit because this is a very vulnerable location for vandalism and tampering.

Camera mounts should be selected to handle the weight of the camera, lens, and housing. A good rule of thumb is to select a mount that will handle twice the weight of the load as calculated from the specification sheets of the selected components. Mounts are usually specified as indoor or outdoor mounts. A mount designated for installation outside also can be used for interior installations, but an indoor mount should not be used outdoors. Outdoor mounts are treated for corrosive effects not normally encountered indoors (although one common exception would be in a high-humidity area such as an indoor pool). Some mounts have separate mounting bases and must be selected for either suspended ceiling or solid wall/ceiling mounting locations. Pole mount brackets are available for some outdoor camera mounts. The mounts should have adjustable heads to allow for up/down and sideways adjustment of the camera field of view. Mounts also come in different lengths, and this may be a consideration when a camera housing adds to the length requirement. Primarily, the mount should be rigid enough and mounted securely enough to the surface so that the camera does not vibrate under normal operating conditions.

Many camera manufacturers and distributors also carry a full line of camera mounts, as well as housings for their cameras. Mounts are priced anywhere from approximately $30 to $150.

11. Lighting requirements and nighttime applications

Most schools generally will not attempt to use exterior CCTV cameras during the nighttime because of the high light levels that are required.

For exterior nighttime CCTV applications, proper lighting is very important. A number of lighting types are available. These types include incandescent, fluorescent, and high-intensity discharge. Incandescent lighting is the most expensive to operate and includes the flood or quartz lights that are commonly used for exterior home security applications. Most fluorescent lighting is used indoors for office and work area lighting. High-intensity discharge lighting is the least expensive to operate (more light is produced with less power consumption) and is the most common for commercial exterior lighting applications. It includes high-pressure sodium and low-pressure sodium lighting. A disadvantage of high-intensity discharge lighting is the restrike time. If a momentary power outage occurs, these lights will go out and can take up to several minutes to return to full brightness. The advantages of high- and low-pressure sodium lighting, however, outweigh this disadvantage for CCTV applications.

Low-pressure sodium lighting is the most desirable choice for exterior CCTV applications because it is somewhat more efficient to operate than high-pressure sodium, and the types of light fixtures available provide a fairly uniform light pattern. A disadvantage to low-pressure sodium is the monochromatic yellow light it produces, which some people find objectionable.

Important items to consider for nighttime camera lighting are illumination level, camera sensitivity, lens type, light-to-dark ratio, area of illumination in the camera field of view, and lighting position. Note: These are not simple issues to be addressed by a neophyte. Be certain that you discuss lighting issues with your local power company or lighting expert.

Illumination level, camera sensitivity, and lens type. Lighting levels must be high enough for the camera to produce a useable image. The light level required will depend on camera sensitivity and lens type and quality. Black-and-white cameras generally have more light sensitivity than color cameras and are recommended for most nighttime applications. A minimum illumination level of 1.5 foot-candles, as measured on a horizontal plane 1 foot off the ground, is recommended for a black-and-white camera with a sensitivity specification of 0.007 foot-candles faceplate illumination. This assumes the camera has a good-quality, F/1.4 fixed focal lens. A color camera or a camera with a zoom lens will require a higher light level in order to get equivalent brightness and contrast.

Light-to-dark ratio. A recommended maximum light-to-dark lighting ratio is 6 to 1 (as measured on a horizontal plane 1 foot off the ground). This maximum applies to the entire area of interest that the camera is viewing. It is also recommended to design the lighting for a 4-to-1 ratio to allow for some degradation over time. A 6-to-1 light-to-dark ratio will prevent areas that are so dark or so bright that a person or object would be obscured.

Area of illumination in the camera field of view. A minimum illumination of 70 percent of the camera field of view is recommended. A camera is an averaging device. If too little of the field of view is illuminated, the camera will average between the illuminated areas and the nonilluminated areas, resulting in blooming and loss of picture detail in the illuminated area.

Lighting position. The position of lighting in relation to the camera field of view is also important. As much as possible, light sources must be kept out of the camera's field of view. Lights that are illuminating a camera scene should be mounted higher than the cameras. When determining a location and field of view for a camera, extraneous light sources, such as building-mounted lighting for pedestrians that will be in the camera view, must be considered. Extraneous light sources can cause blooming and streaking in a camera, rendering portions of the field of view unusable. Distant light sources that are relatively dim are usually not a problem.

Other lighting. Another type of lighting is known as infrared (IR) or near infrared. The spectrum for this lighting is just below red and is not visible to the human eye. Most black-and-white cameras have sensitivity into the infrared. A black-and-white camera can be used with this type of lighting to observe areas at night without having lighting that is visible to humans. To make use of IR lighting, the camera must not have an IR cut filter. Cameras can be ordered without IR cut filters; be sure to specify no IR cut filter when ordering.

Commercial IR light sources include incandescent and the light emitting diode (LED). The incandescent type typically use a 300- to 500-watt lamp and a visible light cut filter. These are expensive to purchase ($800–$1,200) and expensive to operate and maintain (2,000 hours is a nominal life expectancy of the incandescent lamp). The LED type emits light in the IR and is also expensive to purchase (around $1,200) but uses less power and has a much longer life expectancy. The incandescent type will provide more illumination than the LED type. With either type of IR light, more light fixtures will be required to illuminate an area than with visible lighting. While IR lighting has the advantage of not being visible to humans, it is fairly expensive.

Alternatives to lighting. There are two camera technologies that can see at night without the use of artificial lighting. These technologies are intensified cameras and thermal cameras, though they are probably both cost-prohibitive for most schools. Intensified cameras use a photomultiplier (light intensifying) tube in front of the camera imaging device. Depending on the generation of the photomultiplier tube, these cameras can produce a picture in conditions ranging from moonlight to starlight. Disadvantages of these cameras include initial costs, maintenance costs, and lower resolution. Costs for an intensified camera can begin around $8,000. The photomultiplier tube has a life expectancy in the range of 8,000 to 10,000 hours, requiring replacement every 1–2 years depending on the amount of use. In terms of horizontal TV lines, intensified cameras have lower resolution than a good-quality surveillance camera.

Thermal cameras are sensitive to thermal energy radiated by objects. The low-end and minimum-performance thermal cameras start around $7,000. The high-performing thermal cameras range up to $30,000 and require equipment for cooling the thermal imaging device. This cooling equipment can be maintenance intensive. Resolution is also lower than in general CCTV surveillance cameras. Uncooled cameras are currently coming down in price and may offer a better alternative in the future.

12. Covert cameras

There may be times when it is suspected or known that unlawful events, including drug deals, fighting or intimidation, vandalism, or nighttime theft, are occurring on campus. With cameras in plain view, it is clear to all where not to carry out such dealings but; where incidents of concern are out of sight, it may be beneficial to temporarily install a camera hidden from view of the suspects (exhibit 2.13). (Schools should make certain that they consult an attorney before utilizing hidden cameras.)

Cameras hidden from the view of suspects under investigation are referred to as covert cameras. In school applications, these cameras are generally hidden behind a wall or ceiling or within a common building fixture. In some instances, it may be practical to use a normal size, readily available camera if a convenient hidden location is available, such as behind an air duct. It would be reasonable for a school district to have at least one smaller camera available for covert applications.

A whole new industry has arisen in the past few years that specializes in these tiny, easily hidden cameras. These tiny cameras designed for hidden applications are available in black-and-white or color. Microphones are included with some cameras, but caution is advised in their use due to state laws regarding privacy of conversations. An amazing array of disguised cameras already installed within smoke detectors, clocks, speakers, light switches, junction boxes, neckties, caps, and so forth are available in security trade journals; it is then up to the security department to appropriately place the item where it will not be suspicious. The size of available covert cameras themselves measure about 1.25 inches square. The lenses, including pinhole lenses, come in sizes ranging from 2.5mm to 25mm. Covert kits will provide both the camera and a set of several lenses that will handle a wide range of applications, from wide-angle to telephoto. Passive infrared cameras and surface-mount cameras also are available. They can allow surveillance in some low-light environments. Voltage requirements for the cameras are normally 9 or 12 volts dc and can be battery powered.

The video recorder that will be necessary to record the images captured by a covert camera must also be hidden from view. This may not be a simple matter. The smallest video recorder is much larger than the smallest camera. It requires ventilation, a somewhat clean environment, accessibility, and it makes noise. It may be necessary to install the recorder in a separate secure room or even in another building.

The video signal must be transmitted from the camera to the recorder. Coaxial cable is needed for these connections. Wireless covert board cameras are available. Although their use can greatly simplify installation, their transmission ranges are limited to about 300 feet.

Covert black-and-white board cameras start at around $150, with a resolution of about 380 lines. Color covert cameras are close to $300, with a resolution of around 330 lines. For these operations, black-and-white cameras may be adequate or even desired. Many covert situations occur in fairly small areas, and a higher resolution black-and-white camera may be more appropriate than a lower resolution color camera. Cameras already mounted covertly within a fixture can cost between $250 and $500. Wireless cameras can range from $500 to $1,000 or more.

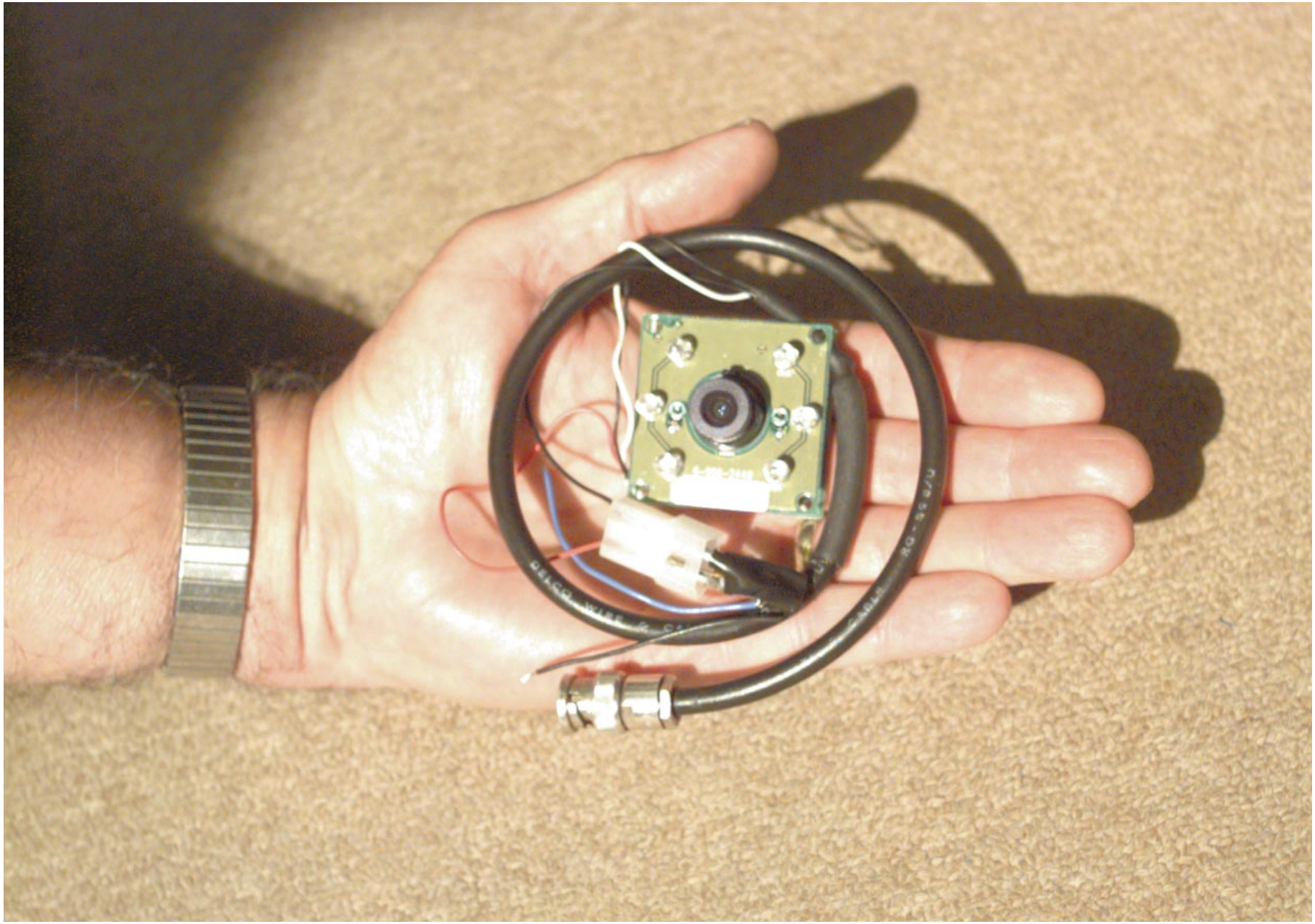


Exhibit 2.13. This shows the relative size of a typical covert camera.

13. Maintenance and expected lifespan

After successful installation, the required regular maintenance of a fixed camera is normally to clean the outside lens. Depending on the strength of the camera's mounting and the stability of the structure it is attached to, occasional repositioning of the camera to correct the viewing angle may be required, especially for exterior applications. (It is not unusual to see one or more incorrectly positioned camera scenes on the monitors of an established security communications room because regular maintenance of camera mountings has not been provided for.)

Housings will protect the camera lens from dust and dirt, but the glass front of the housing must be kept clean. Some super housings come with their own wiper blades and wiper fluid dispenser. The dispenser mechanism is activated remotely by an operator to keep the camera scene clear. However, this feature can add to the required regular maintenance as the dispenser must be refilled with fluid as needed.

The dome enclosures for interior ceiling-mounted cameras (usually pan-tilt-zoom cameras) are intended to reveal the presence of a camera but not its current direction or field-of-view. Dust (or mischief) can obscure the view, but otherwise, maintenance is low.

The average lifespan of a modern solid-state camera is greater than 5 years. Many camera failures occur early in a camera's life. This allows for most cameras with defects to be returned during the warranty period.

Cameras do occasionally need repair, so the availability of parts should be considered. This can make a good deal on an older camera system less fortuitous. If a camera unit used in a critical application must be sent away for repair, it is wise to have a backup camera available. Maintenance contracts should always address repair time and the availability of loaner units.

In the absence of a maintenance contract, there are many local repair shops in most medium and large cities. Check the availability of local repair options before you purchase your system. There are several resources for camera maintenance available to customers across the country who are willing to ship their equipment; repair generally takes less than 2 weeks. Most of these resources may be located on the Web.

14. Price ranges

Standard-resolution solid-state cameras can cost between $300 and $1,000. High-resolution cameras can range anywhere from $1,500 to $8,000. For most school applications, the standard-resolution camera is probably adequate. The less expensive cameras (nearer to $300) need more light to accurately capture a scene. The more expensive cameras ($1,000 or more) tend to be more sensitive, using more sophisticated electronics so that they require less light to accurately capture a scene.

15. Going out on bid for equipment and system maintenance contracts

While it is difficult to prevent every possible mistake when going out on bid for CCTV systems, there are a few commonsense approaches that should be incorporated

in every request for quote (RFQ). The security equipment industry is no different from any other supplier; they will bid on and provide what is asked for. Even generally standard options that would seem reasonable to assume would be included should not be assumed to be part of any RFQ. If you can precisely describe what you require, the bidders will be less apt to submit bids on dissimilar systems.

Do not accept or pay for a camera system until it has been installed and is demonstrated to operate according to your specifications. Remember, the vendor doesn't like surprises any more than you do so specify your acceptance criteria very clearly in the RFQ. This includes the "quality" of installation (exhibit 2.14); occasionally a contractor may try to save money by merely tacking cabling along the top of a wall instead of running the cabling within a conduit and within the ceiling. Don't assume anything.

When going out on bid, the ideal specifications for a CCTV system would describe the desired capabilities or goals of the system, not the quantities of different components. For example, if it is desired to have cameras viewing the locker bay area to discourage and identify daytime thieves, do not request "two cameras, one installed at the end of each hallway." A more profitable request could be: "The images saved to videotape and viewed on the system monitor will allow the customer to distinguish, as a measure of acceptance testing, between the geometry teacher and the school secretary standing anywhere within the locker bay area, with at least one image per camera captured and recorded per second. Quoted product and installation should be vandal-proof, such that an individual, given a few minutes of uninterrupted time, would not be able to vandalize the equipment without being recorded on tape and being identifiable, providing they are not wearing any type of mask." Include room dimensions and even a few photographs of the area for which the requested equipment is intended, or offer all potential bidders a tour of the area.

It is common for the prices received from such a request to be substantially higher than the school originally intended. It is efficient to include a request in the original RFQ for two different camera layouts and their associated costs. One layout would provide the exact capability requested. The second layout would be the best possible configuration within a specified dollar amount, with the expected capabilities as well as deficiencies that are expected with this layout, clearly identified by the vendor. It is to both the school's and vendor's benefit to request these two different layouts—a principal or security official armed with such information can approach the school district or school board to request the additional funding necessary to meet the goals of the security system if the less expensive system will perform substantially below the school's requirements.

Typical warranties on video cameras are 90 days, with up to a year or more for more sophisticated cameras. It is common for cameras that are defective to fail fairly quickly after installation. Be prepared for this; assign a person to be responsible for checking regularly on the functioning of the equipment and to immediately remove failing components and return them to the manufacturer within the warranty period, or to contact the vendor and make certain that he responds in a reasonable amount of time.

Exhibit 2.14. This is an example of a sloppy installation job—be careful how you word a contract for installation.

If a school does desire to have a maintenance contract, either because of lack of internal manpower or because of available funding, the vendor should specify the maximum time it will take to respond to calls for help and the maximum time the customer will have to be without this equipment if a repair is required. It is possible for a school to request faster response times or even that the maintenance contractor provide loaner equipment for any down time greater than 24 or 48 hours; however, this will increase contract costs.

16. Signage for use of cameras on school grounds

Very visible and hard-to-miss signs at the entrances to a school campus and at major entrances into school buildings serve many purposes. Their value to security should not be underestimated. Signs are not overly expensive, but the price of not having one can sometimes be astronomical.

- Signs that inform the public and the school occupants that certain security measures are in force can provide a frontline deterrent. Without any other knowledge, an outsider faced with the choice of vandalizing a school with security warning signs or a school with no signs or other obvious indications of self-defense will choose the latter.

- As described in the section of this manual on legal issues, liability can be minimized through the use of signs. A piece of information that can be important to include on a warning sign is whether cameras are not being monitored. There have been a few lawsuits in the United States that have been filed and consequently won because someone at a facility was attacked, but the victim did not try to defend himself or herself against the perpetrator; he or she was under the impression that, because a video camera was aimed directly at him or her, help would surely arrive soon. This is a common assumption. Sample wording for a school sign regarding this particular issue could be:

  WARNING: This facility employs video surveillance equipment for security purposes. This equipment may or may not be monitored at any time.

- Covert approaches to security can sometimes be open to contention, especially by someone who is caught in this way. The use of covert cameras can be extremely effective in providing evidence for prosecution; however, not all school districts or school boards will support their use. It may not be necessary, however, to post signs regarding every security detail being incorporated on a campus. It may be quite sufficient to insert a warning regarding the use of covert cameras in the school policy document that is signed by every student and parent at the beginning of the school year and in the contracts signed by every employee. (Don't forget to include this information in contracts for outside services.)

17. Legal aspects of the use of video cameras in schools

Laws concerning privacy issues and civil rights may vary widely, so before beginning any electronic surveillance program, be sure to check with your school attorney. However, the following generalities are fairly consistent across most of the country:

Cameras may *not* be used in an area where there is a "reasonable expectation of privacy." Examples of these are bathrooms, gym locker/changing areas, and private offices (unless consent by the office owner is given). Examples of where cameras are generally acceptable are in hallways; parking lots; front offices where students, employees, and parents come and go; gymnasiums; cafeterias; supply rooms; and classrooms. The use of cameras in classrooms is often debated by teachers who want cameras for protection and teachers who do not. At this point in time, it is probably wise to use cameras in classrooms only when the teacher is given an option and notification that a camera is to be used.

Signage can be an important legal component in the use of video cameras in schools. As mentioned in the previous section, it is important that the presence of video cameras not lead a person to believe he or she will be rescued if attacked. Dummy cameras should not be used (which is in contrast to the "black boxes" on buses, in which cameras may or may not be located at any time). While a fake camera can create a temporary deterrent to some security incidents, the potential liability it creates due to a victim's impression of being rescued quickly is not acceptable.

Audio recording is often considered to be of greater legal concern than video recording in most States. The recording of conversations is viewed as more of an invasion of privacy, as conversations often take place where the participants do not expect to be overheard.

B. Video recording equipment

1. VCRs: the weak link

The video cassette recorder (VCR), commonly used in most school surveillance systems, is the weakest link in the video system due to its mechanical nature. (The more reliable but much more expensive digital recorder is discussed later.) Industrial quality VCRs range in price from $500 to $4000. A school can plan to spend approximately $500 to $1,200 for a good-quality VCR appropriate for most of its applications. (This price range does not necessarily include some of the desirable features discussed later.) The inexpensive $200 VCR is not recommended for nonhome use.

Unfortunately, the most ignored maintenance task in most school security departments is the regular servicing and cleaning of VCRs. VCR heads should be cleaned after every 100 hours of use—about every 4 days of constant recording. This head cleaning can be accomplished using isopropyl alcohol and industrial swabs and takes about 10 minutes. The cleaning tapes that are available to clean VCR heads are not recommended, as they can cause excessive wear on the heads. The entire VCR unit should be serviced every 2,400 hours, or about every 3 months of constant use. This complete servicing includes replacement of bands and rubber components. If well-serviced, a typical VCR will last about 4–5 years with constant use. At least one moderately expensive

($200–$300) head replacement should be expected during this time.

Premium-quality tapes are recommended for the constant use experienced in most school applications. These tapes will cost about $10 each and are available from your VCR vendor. Their expected quality lifespan is about 25 recordings. Recording over the same tape indefinitely is not recommended because this practice introduces several logistical problems. Sometimes incidents are reported several days after they occur, and the video of the incident has already been recorded over. A good recording plan includes 6 new tapes every fall and spring, labeled Monday, Tuesday, . . . Friday, and Weekend. Each morning, the appropriate tape is put into the VCR. When an incident occurs, that particular tape should be pulled and labeled as "removed," along with the date it was most recently recorded on. A new tape labeled with that day of the week should replace the original. If faithfully done, this will probably be adequate for most schools. By replacing the tapes every spring and fall, the tape quality is not compromised.

VCRs, which operate at temperatures between 32°F and 104°F, need to be used indoors where relative humidity is less than 80 percent and the air is free of noncondensing moisture. Because an industrial time-lapse recorder is designed to run 24 hours a day for long periods of time, proper physical location of the unit must be considered. Recorders generate heat, and because heat is the worst enemy of the recorder (next to dirt), the recorder must be placed in a well-ventilated location. If the recorder is to be installed in an environment where there is a lot of dust or dirt in the air, provisions must be made to keep the unit clean. (A single grain of dirt in the right place can crack a video head.) If a recorder must be placed in a dirty environment, a housing with a fan, vent holes, and filters should be used.

Another important consideration in setting up a VCR is locating it in a secure, protected area (exhibit 2.15). VCRs are attractive targets for thieves, but even more importantly, tapes can be stolen or destroyed if there is an illegal incident to be covered up. VCRs should usually be placed in a strong locking cabinet within a locked room. Only the school principal and one security person should have the key to this cabinet.

2. Multiplexers

Multiplexers can be used to combine two or more individual video camera signals and send them to a single recorder. This is often referred to as timeshare multiplexing and allows up to 16 video camera signals to be recorded on a single half-inch videocassette simultaneously and played back as individual pictures or combinations of pictures upon command. A multiplexer could be either a simplex multiplexer or duplex multiplexer. The simplex multiplexer can only display a full-screen image of one selected camera or a sequence of selected cameras while recording. A duplex multiplexer can also display multiscreen images while still recording. Essentially, a multiscreen display consists of a split screen that allows for the viewing of all camera images on the system simultaneously (exhibit 2.16).

Timeshare multiplexing can also be used to transmit multiple video camera signals (up to 16) from one point to a second point by a single cable or transmitter

Exhibit 2.15. This video recording equipment is protected by a simple locked and vented cabinet that resides within a locked room.

Exhibit 2.16. These monitors in the principal's office display the camera signals from the main entrance to Belen High School in New Mexico, and allow Ron Marquez to keep tabs on student entry and exit, even while he is in meetings.

(microwave, fiber optic, infrared). Another multiplexer at the second point can be used to separate the multiple video signals back into individual video signal outputs.

A duplex multiplexer is higher in cost than a simplex multiplexer. Generally, a duplex multiplexer is used if someone is watching or operating the system while it is recording; if it is unmanned, as in many school applications, a simplex multiplexer is more cost-effective. A true duplex system allows the user to watch multiple screens while recording without affecting the multiplexed output to the video camera recorder (VCR). A simplex system allows for full-screen or sequenced viewing in the record mode. If multiscreens are activated during the recording, the multiscreen itself might be recorded, thereby not allowing full-screen playback. A duplex system also allows for recording and playback simultaneously if two VCRs are connected. The multiplexer should provide two monitor inputs if this feature is used so live viewing of the facility is not lost. In most applications, a simplex unit is suitable and more economical if recording can be stopped while the video is reviewed. The recorded videotape can then be retrieved in a full-screen or in a multiscreen configuration.

Most multiplexers available from established manufacturers feature camera titling for recording and a permanent time/date stamp on each frame of recorded video.

Another feature is compensation for camera synchronization. Multiplexers are equipped with an alarm input for each camera. When activated, these can be used to generate an output to the VCR to place both the multiplexer and VCR into the 2-hour recording mode (real time) for a predetermined period of time. Some multiplexers allow only images from the alarm camera to be recorded, but others allow a choice of interleaving (every other field). Onscreen programming of the multiplexer allows for simpler programming and review of settings. Programming features should display VCR tables because it is important to synchronize the multiplexer to the particular model and brand of VCR to avoid missing crucial information.

3. Time-lapse recorders

Time-lapse recorders have the ability to incrementally record at specific time intervals, recording a single field or frame of video information with each increment. In the 2-hour (real time) recording mode, a video recorder is recording 60 fields or 30 frames of video information each second. To determine the time interval between pictures recorded at specific speeds, the following formula can be used (based on using a T120 tape at 60 Hz):

$$\frac{\text{Recording speed}}{120} = \text{Seconds between frames}$$

Because the tape is slowed down in the time lapse mode, and the video heads record only specific fields of information, some actions are easily lost. If a tape recorded in real time (2-hour) was compared to a tape recorded at a 240-hour speed, there would be lost information between them. The slower the tape speeds during recording, the more information that can be lost. Exhibit 2.17 presents recording intervals for various recording tape speeds.

There are some low-priced time-lapse recorders (approximately $500) on the market today, but dependability and resolution may be sacrificed if an industrial-quality recorder with at least 400 lines of

resolution (approximately $1,200–$2,700) is not specified. A high-resolution camera and monitor may be used with good results during realtime viewing, but if the playback tape has been recorded with a standard time-lapse recorder with low resolution, the results may be disappointing. For best results, a high-resolution industrial-quality recorder should be used.

4. Event recorders

It may not be necessary to have all the features of a time-lapse recorder. Time lapse was developed to give a continuous flow of recorded information that could span long periods of time in a very small, storable format. If a school is able to interface its intrusion detection or other type of alarm system with their CCTV system (which is viewing the area where an alarm is occurring), an event recorder is capable of turning itself on to record that event almost instantaneously. Not only does this feature allow a tape to be used for very long periods of time, as no recording is being done during uneventful times, but event recorders are generally cheaper than time-lapse recorders.

5. Digital recorders

The security industry now has access to technology that allows the digital recording of full-motion video. Over the next few years this type of system will likely become even more accessible, with an increase in digital storage technology and a decrease in the overall costs associated with hardware. Digital storing and recording have many advantages over a time-lapse or event recorder. The most important advantage is that digital recorders require no human intervention, which means no maintenance and no cleaning. On the other hand, a major disadvantage is that the security industry has yet to establish standards for compressing digital information for recording (compressed digital information takes up less storage space). Hence, it is common to experience compatibility problems between alarm monitoring systems.

For school applications, a major consideration is the increased cost of digital recorders over conventional video recorders. A minimum system for digitally stored images on a hard drive is estimated to cost at least $3,000. Without video compression hard-

Exhibit 2.17.

Recording speed (hours)	2	12	24	72	120	168	240	360	480	600	720
Recording speed (days)	1/12	1/2	1	3	5	7	10	15	20	25	30
Recording intervals per field (seconds)	0.02	0.1	0.2	0.6	1	1.4	2	3	4	5	6

ware/software, the digital storage system is not very practical; it has been estimated that the cost for a single stored image is $0.94 for black-and-white and $2.81 for color. Using the compression methods available today increases the storage capacity with acceptable video quality by approximately 10 times. The additional cost of the compression system is at least $1,500, making the cost of the complete digital recording system about $4,500, which yields a cost-per-image of $0.047 for black-and-white and $0.141 for color video. For comparative purposes, the cost of storing images on a typical video cassette recorder is many times less—each T120 video cassette holds 432,000 black-and-white or color images at a cost of roughly $0.003 per image (including the cost of the VCR).

While the cost of digital storage systems has been decreasing and will continue to decrease as technology improves and the capacity of these devices increases, the cost of tape will probably be much lower than the cost of hard drives for some time to come. Consequently, the security industry will likely parallel the computer industry in storage techniques, using hard drives for short-term storage but keeping archival storage on low-cost tape systems.

Exhibit 2.18. A weapon detection system with x-ray detector for carried items and two portal metal detectors for walk-through.

Chapter III Metal Detection

A. Walk-through metal detectors for personnel

1. Do metal detectors really work?—The basics

Metal detectors work very well—they are considered a mature technology and can accurately detect the presence of most types of firearms and knives. However, metal detectors work very poorly if the user is not aware of their limitations before beginning a weapon detection program and is not prepared for the amount of trained and motivated manpower required to operate these devices successfully.

A metal detection device in school security applications is used primarily to locate undesirable objects that are hidden on a person's body. When a questionable item or material is detected by the device, the detector produces an alarm signal; this signal can be audible, visible (lights), or both. Unfortunately, a metal detector alone cannot distinguish between a gun and a large metal belt buckle. This shortcoming is what makes weapon detection programs impractical for many schools; trained employees are needed to make these determinations.

Metal detectors are usually not effective when used on purses, bookbags, briefcases, or suitcases. There is usually a large number of different objects or materials located in or as part of the composition of these carried items that would cause an alarm.

If you ask the average person what a metal detector does and what property to which it is most sensitive, the answer to the first question would probably be that it is a device that detects only metal. The answer to the second question likely would be that a metal detector is more likely to detect metal objects with heavier mass. Both answers are incorrect.

A metal detector actually detects any conductive material—anything that will conduct an electrical current. The typical pulsed-field portal metal detectors generate electromagnetic pulses that produce very small electrical currents in conductive metal objects within the portal archway which, in turn, generate their own magnetic field. The receiver portion of a portal metal detector can detect this rapidly decaying magnetic field during the time between the transmitted pulses. This type of weapon detection device is "active" in that it generates a magnetic field that actively looks for suspicious materials or objects. A magnetometer, a passive device, was much more in use 20 years ago in the detection of weapons. The magnetometer depends on the Earth's magnetic field—it looks for a distortion caused by the presence of ferromagnetic (attracted to a magnet) material.

Counter to intuition, the mass of a particular object is not significant in metal detection. The size, shape, electrical conductivity and magnetic properties are the important properties.

For example, when a long thin wire is taken through a portal (walk-through) metal detector, and the wire is in any geometry except one in which the two ends (or any two points on the wire) are touching, it will rarely be detected. However, shape this same wire into a closed circle and the metal detector will most likely go off, even though the mass of the wire has not changed.

Delving even deeper into metal detector sensitivity, consider the orientation of an object. Take the same

closed-loop wire described in the previous paragraph. Lay this loop on its side so that it is parallel to the ground. In this configuration, the portal metal detector is less likely to see it, but, if the wire loop is upright and parallel to the side panels of the metal detector, the detector will be much more likely to go off in this orientation.

Some people fear the use of a metal detector on themselves because of the possible side effects of being subjected to the magnetic field. This fear is unfounded; metal detectors emit an extremely weak magnetic field, weak enough to be of no concern even to heart patients with pacemaker-type devices. Indeed, the use of an electric hair dryer subjects the user to a much stronger field than would be received by a metal detection device.

Another widely held belief about metal detectors is that they are a straightforward technology, where the equipment does all the work. This is not true at all. The average first-time consumer will undoubtedly expect a metal detector to be much smarter and more helpful than it can possibly be. A metal detector is only as good as the operator overseeing its use.

In many facilities, the misconception exists that someone known by the operator, such as a fellow employee or a security person, should be allowed to circumvent the system. It must be clearly established that in order to ensure the integrity of any routine metal detection program, everyone must be subjected to the program requirements, including students, parents, teachers, custodial and maintenance staff, security personnel (except for sworn police officers who are required to carry a weapon), school administrators, and visitors. To require less would be counterproductive and prejudicial. Signage can be of great help: a sign at the school entrance explaining the importance of the detectors in maintaining a safe and comfortable learning environment provides policy notification. If a more aggressive approach is needed for a particular community, entry signs could spell out a particular school or district policy that requires the screening of all who enter the school, with access denied to those who refuse.

2. Space requirements and layout

The portal metal detector, also called a walk-through detector, is a stand-alone structure that resembles a deep door frame (exhibit 3.1). The typical walk-through detector will take up a space on the floor about 3 feet across and 2 feet deep. (This does not mean that if you have a 3 feet by 2 feet space at the entrance to your facility you necessarily have space for using a walk-through detector.) The typical height of most portal detectors is around 7 feet. Weight of a unit can vary from around 60 pounds to as much as 150 pounds; however, the awkward shape of most portals prohibits their being easily moved by one person. Portals are generally freestanding and are rarely attached to the floor or surrounding structures. Power requirements are for one plug to a typical 110-volt wall outlet.

The first space factor to take into consideration is where people who are waiting to walk through the portal (scannees) will stand. Ideally, there would be no wait for use of the portal, but this is probably unrealistic in a school environment where the entire population of students will be arriving over a very short period of time. Each school has to determine how many scannees will arrive and at what rate. Most detection programs will need to operate indoors, or at least under some type of

Exhibit 3.1. An illustration of a portal metal detector.

shelter, and most schools are going to want to provide a comfortable environment for those waiting. This usually means that there must be enough shelter for the queue of scannees that might build up at any one time and that they should not be overly crowded. There should also be some way of clearly forming a line for scannees to stand in if they will be arriving at a much greater rate than can be processed; eliminating the opportunity for cutting in line would clearly be important in a school to reduce possible fights.

To avoid sending conflicting signals to the detector, the scannee waiting in line to use the portal next should be kept back 3 feet from the current user walking through the portal. Operators of the equipment and scannees who have already walked through also need to be at least 3 feet from the portal in all directions. (Contrary to a scene in a popular movie of several years ago, a gun thrown along the outside of a metal detector by the scannee before entering the portal and retrieved on the other side after the scannee got through would cause an alarm.) Likewise, if more than one portal metal detector is being used, each needs to be at least 10 feet from the others unless they have been synchronized.

Without very special instructions and limitations for the scannee population, it would be most difficult to conduct a metal detection scanning program with only the use of portals. Hand-held scanners are usually required for use on scannees who have triggered an alarm walking through the portal but who fail to be able to immediately determine what object on (or in) the person caused the alarm. Also, it is highly recommended that any routine metal detection program incorporate the use of x-ray equipment for bookbags and purses because of the ease with which a contraband item or material could be hidden within carried baggage. (See the sections in this chapter on hand-held metal detectors and x-ray equipment for baggage.) This equipment mandates additional space.

Space for the scannee to follow procedures is also required. A person about to walk through the portal needs room to place his or her carried items on the x-ray machine, room to put his or her pocket items (coins, keys, heavy belt buckles) in a special pass-through container, space to pick up these items, and space to turnaround to walk through the portal a second time if necessary.

It is very important that there be neither space nor opportunity for particular members of the population, including employees, to walk around the detection system (exhibit 3.2). Very definitive boundaries must be established to prevent circumvention of the system and prevent passback of contraband, where such prohibited items are handed from outside the screening area to those who have already successfully cleared the scanning process.

In designing the layout of the metal detection system, the composition of surrounding walls, furniture, nearby electromagnetic equipment (such as an elevator), nearby plumbing in the walls, and even metal trash cans must be taken into account. The optimal effectiveness of a portal metal detector can be easily degraded by a poor location, a casually placed metal stool, or the nearby use of electromagnetic devices. See the section about sources of interference elsewhere in this chapter.

In schools, the metal detection equipment and personnel will generally be located directly within the front or

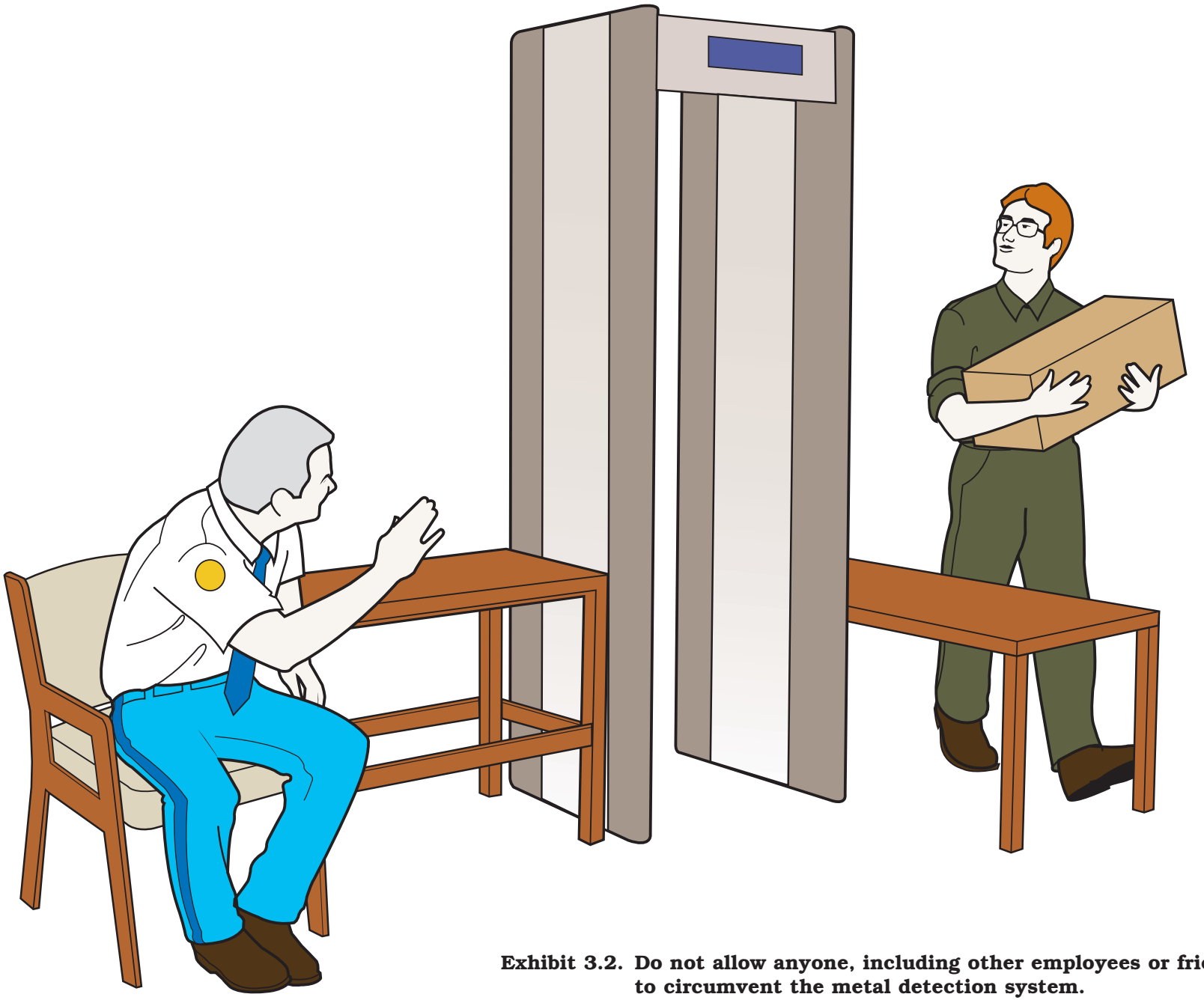


Exhibit 3.2. Do not allow anyone, including other employees or friends, to circumvent the metal detection system.

main student entrance. Unfortunately, the design of most schools does not lend itself to a comfortable staging area for this process. There is usually not nearly enough interior or covered space to allow for all the students waiting to enter the system. This may mandate that the metal detection staging area be located further within the facility, which may place administrative offices outside the cleared area. Conscious decisions must be made and potential risks must be realized when designing the weapon detection program.

A greater problem is often that the layout of schools will not allow for the limiting of only one or, at most two, entry points. Few schools can afford to have multiple entry setups with complete metal detection programs. The cost of the equipment would be quite high, but not nearly as prohibitive as the manpower to run these multiple systems.

3. Throughput

A well-trained and motivated operator should generally be able to process between 15 and 25 people per minute through a portal detector. This does not include investigation of alarms, nor does it take into consideration intentional or unintentional delays that might be expected in a student population.

Assuming that scanning personnel are well-trained, a school's throughput is going to be driven by three things: (1) the number of devices, (2) the rate at which students arrive, and (3) the motivation of the students to cooperate and move through the system quickly and the ability of the school staff to make certain that scannees move along quickly. The breakdown of equipment or the arrival of visitors who are not familiar with the scanning routine will also cause a definite slowdown; the impact of this must also be considered by the school administration but is not taken into account here. (The need for backup equipment must be considered by each facility, whether the equipment is borrowed from the vendor or a pool of spare equipment is shared within a district.)

Keep in mind that any population that is aware that it has to regularly go through the scanning process will soon compensate and adjust their routine. These adjustments will generally be that: (1) the population will attempt to take fewer prohibited items with them into the facility (hopefully), (2) scannees will learn which otherwise acceptable items in their possession will still cause an alarm and will tend to shy away from these items (except maybe in the case of students who wish to create a hassle and who are undaunted by any consequences for doing so), and (3) the population will allow for the additional few minutes in their schedule, perhaps even going so far as to come early enough to miss the main rush. Travelers flying out of busy airports know to allow for a few minute delay at the metal detection scanners and will not cut their arrival time so close that they miss their flight. Students will do likewise, whether they need to show ID cards at the front gate, go through a metal detection system or meet with their friends before class. However, unreasonably long waits of 15 minutes or more could result in staff, students, and parents alike reevaluating the need for a metal detector program. Nobody wants to add significantly to their workday, especially if they are not compensated for it. Employee organizations may bargain for extra pay for this additional at-school time.

Exhibits 3.3 and 3.4 depict the average number of students that would be waiting at each 5-minute interval

before school to enter the weapon detection system for a school population of 1,000 and 2,000, respectively. For these calculations, it was assumed that metal detection equipment is in good working condition and optimally laid out, operators are motivated and comfortable in their tasks, and students move smoothly through the process. The arrival rate resembles a school morning where the bulk of students arrive within a 10- or 15-minute window, perhaps resembling a school whose students rely primarily on buses for transportation. (Whether or not the assumed arrival rate is truly typical of student arrival times is unknown; its use here is for enlightenment purposes only.) The overall throughput is gauged in terms of the number of students who will be waiting to enter the metal detection process at any particular time. The assumption is made that the portal metal detector will be the bottleneck of the scanning process and that other supporting components of the detection program will be able to perform their functions in an equal or lesser amount of time (although this may not necessarily be true at a particular school, depending on its setup). It is also assumed that the process will be set up such that students who fail the initial portal screening will be immediately funneled to an alternative screening point and will not have to reenter or further delay those at the main entry portal.

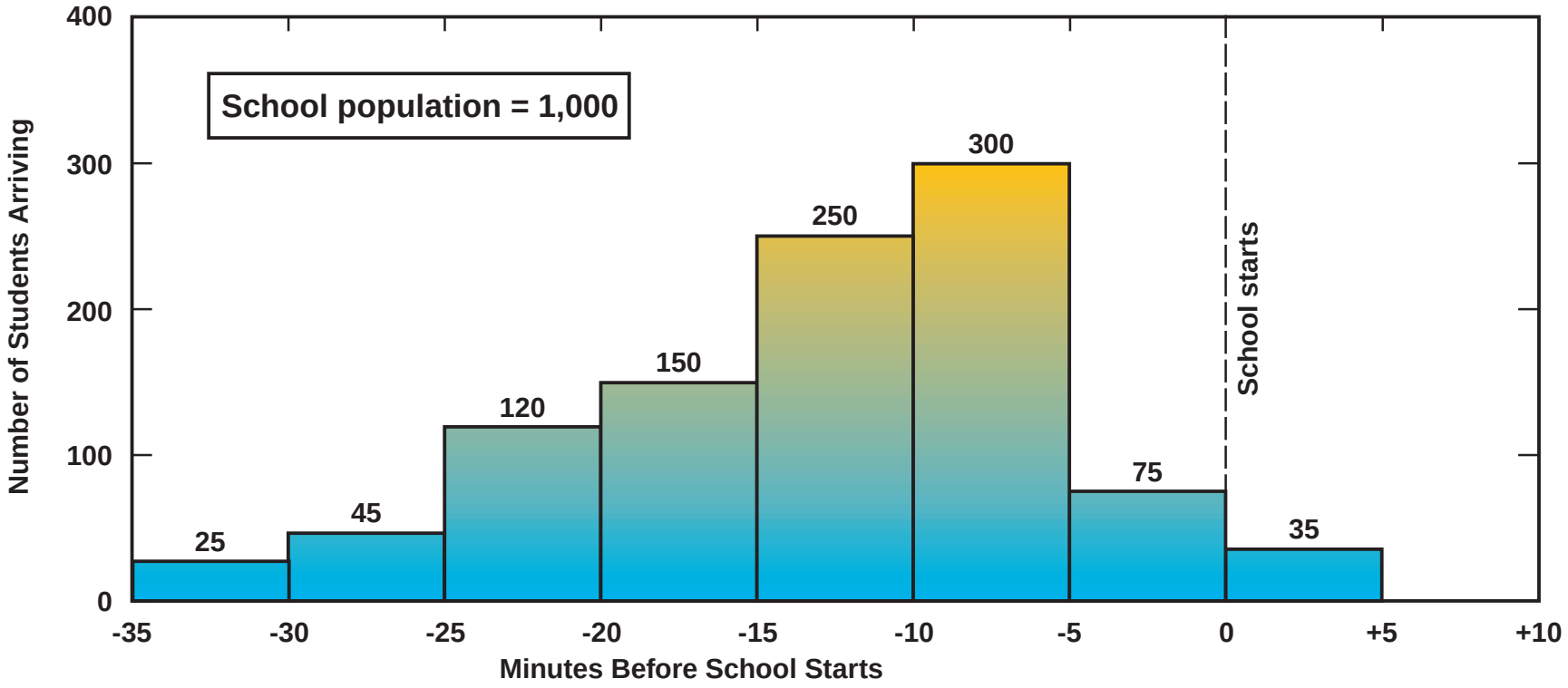
For students prepared to clear the portal who have minimized alarm-causing items and materials in their possession, the actual processing time through a metal detection program should be less than 10 seconds. For students who are not prepared, the processing time may add an additional 3–5 minutes or more for scanning the body with hand-held metal detectors and/or manual bag searches. This does not include the additional delay of waiting to be scanned.

After carefully calculating the necessary metal detection equipment, space, and personnel, and making adjustments for individual school characteristics, the administration may realize that there simply aren't enough resources available to handle its students in an acceptable manner. Some schools have overcome these limitations by staggering the schoolday start times for students, thereby spreading out the school's limited metal detection resources. Unfortunately, schools that rely heavily on bus service may not be able to utilize this solution.

4. Hardware costs and manpower costs

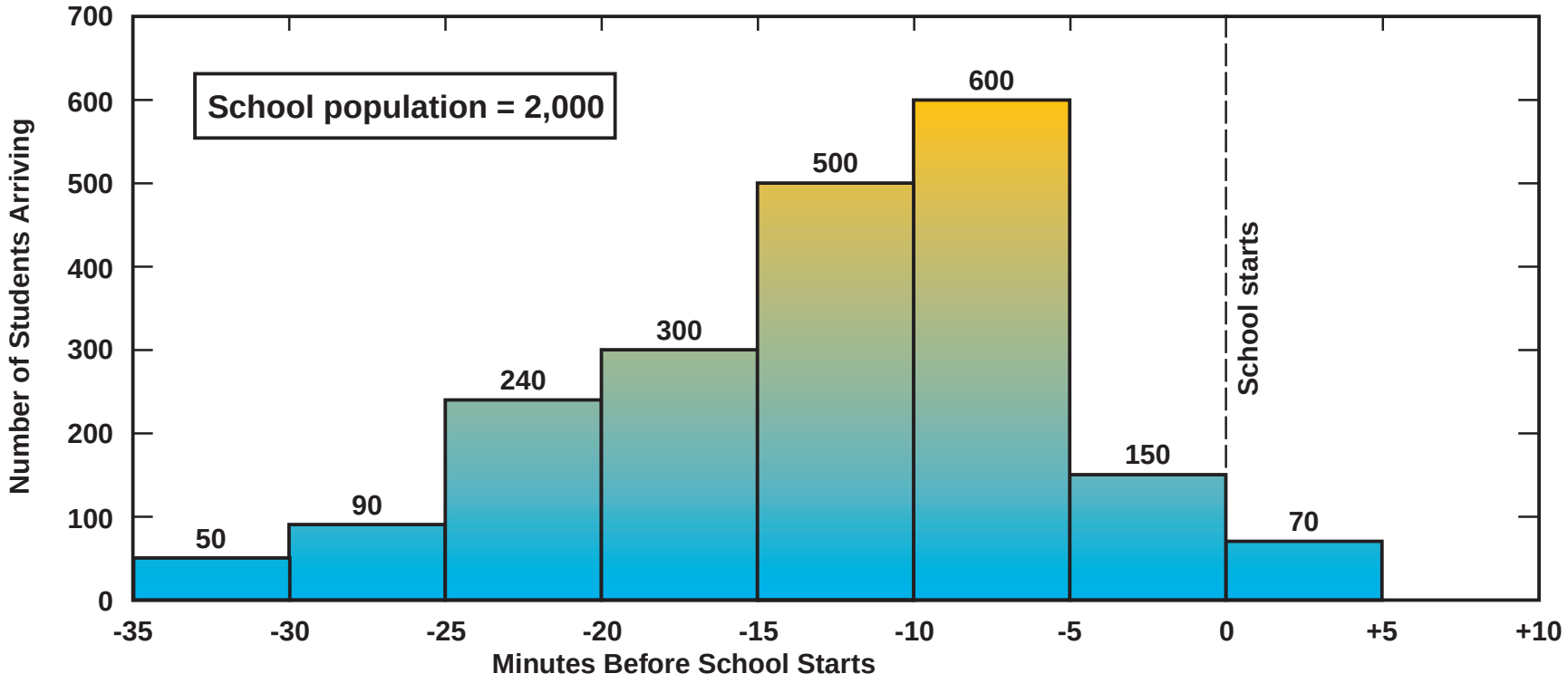
Portal metal detectors vary widely in price. Portals on the market range from as little as $1,000 up to as much as $30,000. The moderately-priced models around $4,000 to $5,000 probably offer the features and reliabilities required for a school metal detection program. Models closer to $1,000 are not recommended due to lack of sensitivity of these devices. Models in the higher price ranges generally offer enhanced capabilities that would not be necessary or warranted in a school environment.

The initial purchase price of a portal metal detector is almost insignificant compared with the ongoing personnel costs to operate the equipment in a complete weapon detection program. An excellent example that illustrates this fact is the successful weapon detection program run by the New York City (NYC) Board of Education in about 50 of its inner-city high schools (exhibit 3.5). For just one of its schools with about 2,000 students, the weapon detection program requires 9 security officers for approximately 2 hours each morning. Two officers run the two initial portal metal detectors, two officers run the baggage x-ray



Number of Students Waiting (Scan time—15 scannees per minute per portal)										
1 Portal	0	0	0	45	120	295	520	520	480	405
2 Portals	0	0	0	0	0	100	250	175	60	0
3 Portals	0	0	0	0	0	25	100	0	0	0
Number of Students Waiting (Scan time—25 scannees per minute per portal)										
1 Portal	0	0	0	0	25	150	325	275	185	60
2 Portals	0	0	0	0	0	0	50	0	0	0
3 Portals	0	0	0	0	0	0	0	0	0	0

Exhibit 3.3. Calculation of number of students waiting to enter weapons screening system using an example arrival rate for a school of 1,000 students. (These numbers reflect ideal conditions; see text for additional information.)



Number of Students Waiting (Scan time—15 scannees per minute per portal)										
1 Portal	0	0	15	180	405	830	1,355	1,430	1,425	1,350
2 Portals	0	0	0	90	240	590	1,040	1,040	960	810
3 Portals	0	0	0	15	90	365	740	665	510	285
4 Portals	0	0	0	0	0	200	500	360	120	0
Number of Students Waiting (Scan time—25 scannees per minute per portal)										
1 Portal	0	0	0	115	290	665	1,140	1,165	1,110	985
2 Portals	0	0	0	0	50	300	650	550	370	120
3 Portals	0	0	0	0	0	125	350	125	0	0
4 Portals	0	0	0	0	0	0	100	0	0	0

Exhibit 3.4. Calculation of number of students waiting to enter weapons screening system using an example arrival rate for a school of 2,000 students. (These numbers reflect ideal conditions; see text for additional information.)

machines, one officer runs the secondary portal metal detector for students who fail the initial detector, two officers (a male and a female) operate the hand scanners on students who fail the secondary metal detector, and two officers keep the students flowing smoothly and quickly through the system, such that nobody is able to bypass any part of the system. It should be noted that the only way these schools are able to avoid huge waiting lines, even with this much equipment and this many officers, and still get everybody to class on time is by a complete restructuring of their class periods. There is a significant staggering of first period start times so that the students arrive over a 90-minute period. On average, NYC school safety officials estimate that they fund approximately 100 additional security officer hours a week for each of their schools that screen for weapons.

To make any metal detection program effective, school access during the rest of the school day, during off-hours, and during special activities needs to be tightly controlled. A motivated student can defeat a lax system. If there is a comprehensive metal detection program at the front entrance to the school, but the back entrance through the cafeteria is unguarded, the funding and efforts put into a well-meaning program can be wasted. A successful metal detection program cannot be poorly funded or run by an administration that is reticent to make major changes to school policies and procedures.

5. Procedures for the operator

The vendor of a particular portal metal detector will provide training and procedures that are geared toward the operation of its equipment. In addition, each school will need to develop specific procedures and policies as to the logistics of its metal detection program. This will include how to process or direct a student who has caused an alarm. The rest of this section will familiarize a facility with what to expect and to provide some general recommendations.

Once a portal metal detector has been set up and has been demonstrated to operate accurately in its current position and with its current settings, the operator will not be required to adjust the control settings. The operator of the portal should be aware of the possible sources of interference with the equipment; something as seemingly insignificant as setting a metal trash can alongside the portal metal detector after it has been put into operation can introduce an area of less sensitivity within the scanning area of the equipment. (See the section on sources of interference.)

Some points for the operator to be aware of are:

a. Do not allow the scannee to proceed through the portal too fast. Ideally, drawn footprints can be located at the base of the portal within the scanning zone. The operator should insist that each scannee actually place his or her feet on these footprints before proceeding. This will ensure that the scannee has not gone through the portal so fast that he or she could have been inadequately scanned.
b. Make certain that no other person is located within a 3-foot radius of the equipment while a scan is being performed. This includes the operator, unless he or she is devoid of any metal on his or her person.
c. Provide a rescan of any person who causes an alarm, even if he or she is able to identify what must have caused the alarm, such as a belt buckle or necklace. Confirm that this person no longer causes an alarm after the offending item is removed from his or her possession. (Particular programs may provide for a second, more sensitive

Photo by Chester A. Higgins Jr.

Exhibit 3.5. A photograph of a successful, but manpower-intensive, weapon detection program at a New York City high school.

scan to be performed by a different portal or by a person with a hand-held metal detector rather than by the original portal.)

d. Do not allow anyone on the outside of the cleared area the opportunity to hand something to a person who has already been cleared by the portal on the inside of the cleared area (exhibit 3.6).

For a portal metal detector that is located semipermanently in one position, the operator will need only to turn the equipment's power switch on, wait approximately 10 seconds for the unit to warm up, and do a quick performance test (see the section on acceptance testing and performance testing). This process should take less than 5 minutes each morning. For a portal metal detector that is moved into position each morning and put away afterward, more extensive procedures will be required. The equipment vendor will be able to give the school good advice as to what additional morning routines will be necessary.

6. Instructions for the scannee

The instructions provided to students, employees, and visitors need to be as short and simple as possible. The following example instruction set could be provided to students and employees in the student handbook and should be posted at the entry to the weapon detection area.

a. Remove any metal items from your body or pockets and put them in your purse or bookbag.
b. Place hats, carried jackets, purses, bookbags, and briefcases on the conveyer belt for the x-ray machine (or on the table to be searched by an officer).
c. Stay back from the portal until signaled by the operator to proceed.
d. Walk at a moderate pace through the portal, one person at a time, being sure to momentarily place your feet on the footprints at the base of the portal before proceeding.
e. If an audible alarm sounds as you go through the portal, follow the directions of the security officer for further scanning or search.

7. False alarms

No portal metal detector is manufactured with the correct adjustments that meet all users' needs. These adjustments or settings are generally made by the vendor when the detector has been installed in the area where it will ultimately be operational. Given equivalent environments, however, different facilities have different requirements for equipment sensitivities. A metal detection program in the U.S. Treasury Department will have very different equipment settings than a program for a school weapon-detection portal. The optimal settings for each facility will be a set of tradeoffs that balance false-positive errors against false-negative errors.

A false-positive error occurs when an alarm occurs for an otherwise acceptable item, such as a metal key ring. These errors occur more frequently in a program that seeks to err on the side of security. False positives can be extremely annoying to scannees and can increase the manpower required to support a metal detection program. Constant false-positive alarms can also cause the operators of a system to become desensitized to alarms, so that they eventually fail to fully investigate the sources of all alarms.

A false-negative error occurs when no alarm is triggered by an unacceptable item, such as a weapon. These errors may occur more frequently in a program

Exhibit 3.6. "Passback" of a weapon from someone outside the facility to a person who has already cleared the scanning process is a common defeat method.

that seeks to err on the side of convenience. A system set more toward false negatives can slightly increase the risk of a weapon entering the facility but generally helps a metal detection program to run as smoothly and quickly as possible. In such a program, when an alarm does occur, the operators will be more likely to take it seriously and to investigate fully what caused the alarm. Many school system programs will be set in this manner.

Most portal metal detectors are additive; they will generate an alarm based on the total response received from the metal detected on a scannee. An alarm does not necessarily mean just one suspicious item has been detected. Because of this, a scannee who has multiple "borderline" items on his other body has a better chance of causing a false alarm. See exhibit 3.7 for a pictorial description.

Item	Source of an alarm?
Most boots with steel shanks	Yes
Orthodontic braces	No
Orthodontic braces with head gear	Borderline
Zippers in clothing	No
Underwires in brassieres	No
Large closed-loop earrings	Yes
Small closed-loop earrings	No
Large loop earrings that are not a complete circle	Borderline
Glasses (for vision) with metal rims	Borderline
Soda can	Yes
Keys	No
Key rings	Borderline
Three-ring metal binder	Yes
Musical instruments and cases	Yes
Foil gum wrappers and cigarette packages	Borderline

8. Sources of interference

Even the best portal metal detector will fail to operate properly if it is not located in an area that minimizes outside interference. There are many different shapes and forms of interference to a metal detector. School administration and security staff should be aware of potential problems. Below is a partial list of possible interference sources (see also exhibit 3.8):

- A metal stool or metal trash can placed close to the portal.
- Fluorescent lights located directly above the operating area of the portal and within 1–2 feet of the top of the portal.

Typical Portal Metal Detector Sensitivities

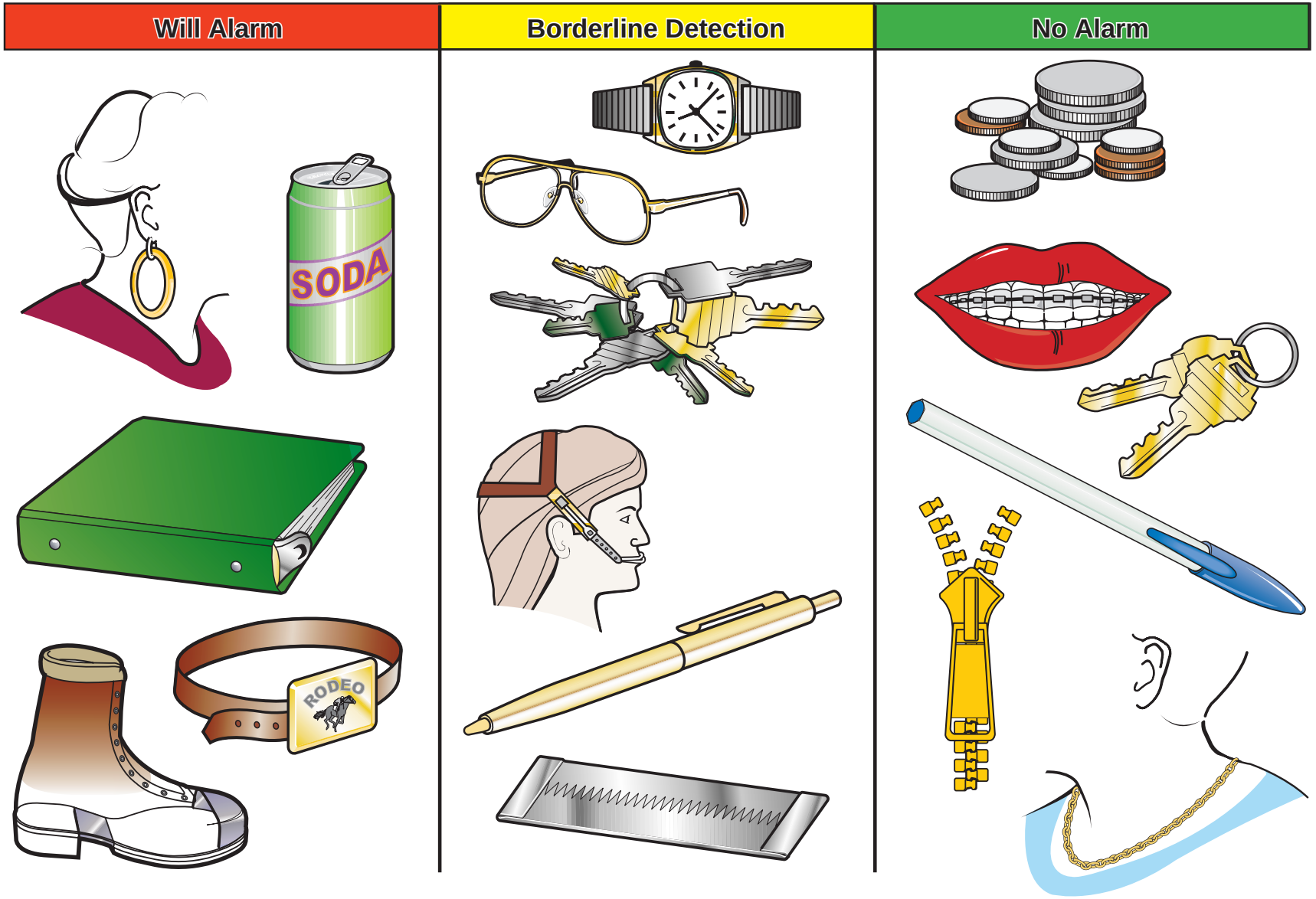


Exhibit 3.7. This drawing illustrates items that are normally accepted, rejected, or whose chance of causing a false alarm will depend upon the particular metal detector used and how it has been programmed.

Exhibit 3.8. Portal metal detectors are subject to many sources of interference that can reduce their sensitivity if not compensated for in the initial programming.

- Motors or anything that causes a spike of electromagnetic energy nearby (within a few feet).
- An elevator motor. If it is a large motor, the elevator can cause interference even up to 10–15 feet away.
- Nearby air ducts in the wall with metal components that expand/contract slightly when the cooling/heating system is in operation.
- Plumbing within a nearby wall such that the pipes vibrate when water is running through them.
- Chain link fencing.

Most nearby metal structures will not prohibit use of a portal metal detector. However, the instrument sensitivities of the detector should be set to allow for the presence of these structures. Any change in position of the portal in relation to nearby metal structures can affect the equipment's sensitivity.

9. Acceptance testing and performance testing

Acceptance testing is a series of rigorous trials designed to determine if a walk-through metal detector is accomplishing what is expected of it. This series of tests is performed after installation and must be repeated after any relocation of the equipment or change to the surrounding environment. The vendor of each particular type of portal will have a series of tests to be performed after setup. Vendor tests are designed to aid in determining the ideal sensitivity settings of the equipment for a particular location and the contraband items of greatest concern. Each school should also have a series of rigorous tests that it will run before accepting or paying for any piece of equipment. The same set of tests can be used by the school later if there is any change to the equipment's environment, especially if the school cannot afford to bring the vendor back in to support them later.

A series of acceptance tests can be devised with knowledge of the weapons that are likely to be present in any particular community. (This threat varies widely in different parts of the country and can change over the years. As no facility can protect itself from every possible weapon in existence, the local law enforcement agency or the school's security department can help determine the most likely threats for that area.)

1. Determine the three or four most likely weapons for a particular school.
2. Obtain replicas or equivalent-composition and similarly shaped items for each of these weapons from the vendor, local law enforcement agency, or school security department.
3. Place these items one at a time on the body of a tester who will walk through the portal with the item placed in various hard-to-detect locations. Conduct about 20 walk tests per location per item. Good locations to test include: the hand, and stuck up into the sleeve, stuck into a sock on the exterior of the leg, stuck into the inside front of the belt, and hidden inside a baseball cap. (Note that this amounts to 20 different trials for each of four different weapons for each of four different body locations—a total of 320 trials.)
4. Determine the three or four most likely borderline items that are acceptable items to bring into the school but that may cause an alarm.
5. Place these items one at a time on the body of a tester who will walk through the portal with the item placed in typical locations—i.e., glasses on face, pocket change in pocket, necklace around the neck. The tester should walk through 20 times with each item.

A particular portal may be said to be accepted when at least 19 of each of the 20 walk-through tests for each weapon results in an alarm, and at least 19 of each of the 20 walk-through tests for each acceptable item does not result in an alarm.

In contrast, a performance test is a much shorter and simpler set of trials that should be conducted by the operators of the system at the beginning of each morning before the equipment goes into operation. This test may consist of walking through the portal four or five times with a piece of metal on different locations of the body. If the portal goes off on each walk-through, then the system is said to be performing well and is ready for operation. If the system fails these tests, and no obvious reason for these failures is evident, such as the recent relocation of a metal object next to the portal, the vendor should be called, and the device should be taken out of operation until serviced.

10. Maintenance and expected lifespan

A good portal metal detector is generally quite reliable and unlikely to need much repair after it is installed and found to be performing well, other than for accidental or careless damage to the equipment. Because of this, the warranties that come with the equipment are probably all that is needed; a maintenance contract is probably not necessary. (Performance tests need to be run on a regular basis. See the section on acceptance testing and performance testing.)

A portal metal detector can be expected to have a fairly long life, probably ten years or more. The useful life of the detector will more likely be limited only by newer and better technologies available on the market in subsequent years.

11. Working with the vendor

Vendors of portal metal detectors may be willing to come to a school with the equipment and perform a demonstration. After the vendor has set up the portal, preferably in the area the school is considering for the ultimate placement of the equipment, and the device's own internal diagnostics and acceptance tests have been run, the demonstrator should be told to set the sensitivities to what he or she considers to be the optimal settings. After this point, the demonstrator should not be allowed to adjust these settings further. (If allowed to constantly readjust the equipment, a less scrupulous demonstrator could constantly reset a device with the knowledge of what is to be the target for each test, such that each target is detected or not detected, as desired.) The school would then run its own set of tests to determine the sensitivities of the equipment. This should include walking volunteer students through with weapon replicas and walking students through who have normal borderline items on their body. (See the section on items that can cause false alarms.) After two or three such demonstration sessions by different vendors, most law enforcement agencies or school security departments will develop a

familiarity with portal metal detector features and what their own application may require.

When issuing a bid for a portal metal detector, a school should require in the RFQ that a bidder meet a series of performance tests, such as those defined in the section on acceptance testing and performance testing. The vendor who is chosen must be required to set up his equipment where desired at the school and then meet the required performance tests. It should also be specified that the vendor will not be paid until these requirements are met. Language in the contract should allow the school to withdraw the contract if the chosen vendor fails to meet these obligations within 2–3 weeks after initial installation.

B. Hand-held scanners for personnel

1. The name of the game: Policies and procedures

Battery-operated, hand-held metal detection devices are a very viable technology for use by schools, and most detectors on the market work quite well (exhibit 3.9). By moving the wand of a hand-held metal detector around and close to a scannee's body, the operator can fairly accurately locate sources of metal (or more accurately, sources of conductive materials) that may be on, or even in, a person's body. When a suspect area is located, the hand-held device will generally give off an annoying squeal. These devices do not have the ability to discriminate between an actual weapon and some piece of benign metal. The responsibility of the operator of the device is to judge whether the squeal he or she heard is truly suspect, then to investigate and determine the cause of it. A very common use of hand-held metal detectors is in airports, where these devices allow the security staff to more accurately locate the source of an alarm on a scannee's body, after a scannee has already walked through a portal system and caused an alarm.

Although most hand-held metal detection devices on the market work well, the hand-held metal detector is only as good as the operator using it. Some vendors and users of hand-held metal detectors say that there are only three things that need to be considered for their successful use: procedures, procedures, and procedures. A disinterested or unmotivated operator can negate much of the benefit that could be derived from a school's metal detection program. While it is not difficult to learn to use a hand-held metal detector correctly, school administrators should not underestimate the value of annual training for their operators, as well as training for staff who may be called upon to serve as backup or supplemental operators. A complete training course, including practice time, should take no more than an hour. However, on-the-job practice is definitely key in allowing the school to achieve the throughput that will be required to process students quickly.

Policies and logistics for use are also very important. Though hand-held metal detectors are affordable, it would be unusual for a school of any size to screen all students and employees each morning using only hand-held detectors. Manpower would be far and away the major cost of such an endeavor. Using a throughput rate of about two students per minute, a school would need one operator for a full hour for every 120 students. This assumes the students' arrival rate is evenly spread across 1 hour, which is not very likely.

If a school is attempting to do a complete screening of students each morning, the hand-held metal detector will more likely be used as a supplement to portal metal detectors. As in airports procedures, the hand-held detectors allow the security staff to more accurately locate the source of an alarm on a student's body, after a student has already walked through a portal system and caused an alarm.

Most schools that desire to establish some type of weapon detection effort (but less than a full-scale, every-morning, every-person effort) will set up a policy to allow random spot checks on students or complete student population scanning as deemed necessary. It is very difficult to do truly random checks with any hope of locating weapons. There is almost always a small but distinct group of kids that a school is most concerned about possibly carrying a weapon. These high-risk students are going to object if you search them more than once, and they would quickly compensate for this anyway, by forcing another student to carry their weapon

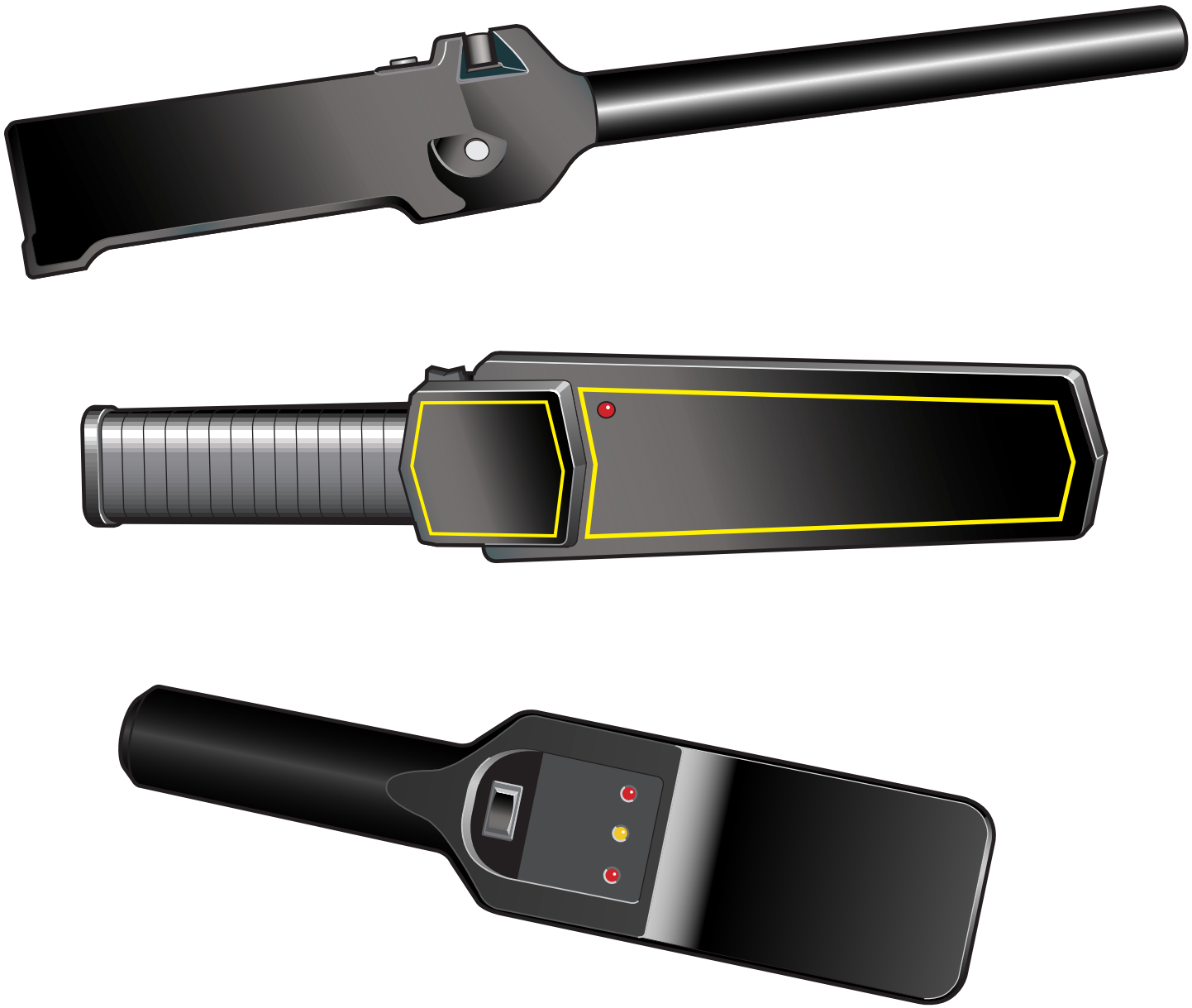


Exhibit 3.9. Examples of hand-held metal detectors.

onto the campus for them. One of the more successful approaches being used is for a school administration to choose an entire classroom at a time and scan every person (including the teacher) in the room.

Complete student population scanning with only the use of hand-held detectors can be undertaken when a school feels that major weapon issues are evolving suddenly and quickly, i.e., a member of the school staff has received information from a reliable source. The school administration and staff need to realize the great amount of time this will take and be prepared to handle the discipline of the crowd of waiting students.

One approach that may help some schools is to establish a policy that allows the school to do a weapon detection scan of any student who arrives at school late in the morning. This may provide the school with a lot of leverage. There could be some excellent deterrence created if students knew they would definitely be scanned when they are running late, if only to convince them to not be late.

It would also be beneficial for information regarding the potential use of metal detectors at school events to be printed on all tickets for games, dances, and so forth.

A school should seriously consider having both a male and a female operator of hand-held detectors in order to perform scans on students of both genders.

2. Space requirements

The use of hand-held metal detectors requires only slightly more space than that already occupied by the operator and the scannee. Unlike portal metal detectors, hand-held metal detectors are not nearly so sensitive to their surroundings; their sensitive zone is usually within just a few inches of the device's paddle. Metal walls, elevators, fluorescent lights, and plumbing that can affect portals do not usually have any affect on hand-held devices. The school must provide enough space for the students who are waiting to be scanned and about a 6- by 6-foot area for the actual scanning process. It is also necessary to have a table or other stable structure for students to place their purses and bookbags on and for them to lean on when they lift their shoes to be scanned. (See the sections about procedures for the operator and instructions for the scannee.)

It is not recommended that this scanning process take place in a private room or area. To avoid possible misconduct, accusations of misconduct, or a confrontation with a student who does end up actually having a weapon, all of the weapon detection program functions should be performed in view of everybody else. The exception is the unusual circumstance wherein a person is suspected of hiding some type of contraband in a private area of their body.

3. Throughput

In an environment where scannees are unfamiliar with the routine of hand-held metal detector use, such as at a courthouse, accurately scanning an individual may take as much as a couple of minutes to do well, especially when there are multiple alarm sources on one person, i.e., belt buckle, pocket knife, and steel shanks in boots. However, in a school environment, after the program has become routine, and where the students are generally cooperative and anxious to get through the metal detection system quickly, it should take no more than about 30 seconds to scan an individual with a hand-held detector. Assuming there are no difficult or

ambivalent students, most schools can plan to hand scan two students per minute per operator.

A good routine for any school weapon detection program involves training the student, staff, and parent populations. If the program requirements are repeated in presentations, in classrooms, and in writing, it will take much less time to settle into a routine. Instructional posters located at the scanning equipment should include diagrams of how a scannee should stand. For a complete, full-scale metal detection program to be held every morning for every member of the school, about 1–2 weeks will be needed for students to acclimate themselves by coming a few minutes earlier and wearing clothing and accessories that are less suspect. The first week of any metal-detection program will be chaotic.

4. Hardware costs and manpower costs

Most hand-held metal detectors on the market range from about $20 to about $350. Schools should plan to spend between $150 and $200 for detectors that have desirable features, including a long detection paddle (to reduce the amount of passes necessary across a person's body), a warning light or beep when the batteries are beginning to run low, and an audible feedback alarm that squeals louder or changes pitch for larger suspicious items and softer for less suspicious items (such as a zipper). Even the least expensive detectors will work, but more time may be required to perform a complete scan, and the procedures for the scan may be more intrusive. These smaller detectors are convenient if a school administrator or security person wishes to carry a smaller detector on their belt at all times.

Hand-held metal detectors run on either a 9-volt battery or on a rechargeable NiCad battery. A new or freshly recharged battery will last for approximately 1 hour of constant scanning. The rechargeable units may require that the battery be recharged by itself. Other hand-held detectors have a jack or plug built into them so it is unnecessary to remove the battery to recharge. (It is suggested that, for hand-held detectors that are used very infrequently, such as once a month, batteries should be removed when the unit is not in use.) A staff member should be assigned the responsibility for recharging batteries each night and/or making certain that new batteries are always available.

Obviously, manpower costs drive the use of hand-held metal detectors. As mentioned in the section on throughput, a trained operator can scan approximately two people per minute. For each operator and all back-up operators, a thorough training course along with some practice time should take no more than an hour at the beginning of each school year. A school should not forget to formally train security personnel who are hired after the start of the school year. (Some metal detector vendors provide an instructional videotape that can be useful, but the tape should not be used as the only source of initial training and practice.)

5. Procedures for the operator

While it is not difficult to learn to use a hand-held metal detector correctly, school administrators should not underestimate the value of annual training for their operators, as well as training for staff who may be called upon to serve as backup or supplemental operators. However, on-the-job practice is important in allowing the school to achieve the type of throughput that will be required in order to process students quickly.

Every school will want to tailor its own set of operator procedures to take into consideration its students' and community needs. Some generic procedures:

- The detector should be passed over the scannee's body at a distance of no more than 3 to 4 inches. Avoid touching the body or clothing with the detector. However, for some baggier clothing, such as pants or jackets, it may be necessary to hold the detector against or more into the fabric while scanning in order to stay within 3 to 4 inches of all body surfaces.
- Most hand-held metal detectors should be set at their highest sensitivity. An exception to this is if there is significant interference from metal reinforcing in a floor or other nearby material that could cause constant alarms unless the detector's sensitivity is turned down.
- The body scan should be performed each time in the same pattern so that the operator always knows what parts of the body still need scanning. A sample routine, illustrated in exhibit 3.10, follows:
  1. Ask the scannee to place all carried items, plus any caps or headgear on a table (procedures for manual search of baggage are not covered in this text). The scannee should stand with his or her feet about 18 inches apart, facing away from the table and about 2 feet in front of it. Footprints outlined on the floor or drawn on a mat can greatly help position the scannee properly. Ask the scannee to hold his or her arms out to the sides, parallel to the floor.
  2. Quickly run the hand-held detector across some piece of conductive material on your own body, such as a belt buckle. The ensuing squeal of the detector will assure you that the scanner is still operating properly.
  3. Start at the top of one shoulder of the scannee. With the paddle of the detector held horizontally and parallel to the front of the body, sweep down one side of the front of the torso, down the leg to the ankle, then move to the other ankle and sweep back up the front of this opposite leg and torso, ending with the opposite shoulder. (If a particular detector's detection paddle is less than half the width of the average body, or if a particular body is wider than twice the width of the detection paddle, the pattern will have to be modified to achieve adequate coverage.)
  4. Sweep the detector paddle over the outside top of the arm from the top of the shoulder to the bottom of the wrist, then up the inside of the arm to the armpit. Sweep down that side of the body to the ankle, then up the inside of that leg and down the inside of the opposite leg, then back up the other leg from the ankle to the underarm. Repeat the sweep of the inside and outside of this arm. Note that it would be particularly important to avoid touching the paddle up against the scannee's body when scanning up and down between the legs.
  5. Ask the scannee to turn around. (Arms can be put down now.) The pattern used to scan the front of the body should now be repeated over the back of the body.
  6. Ask the scannee to grab the edge of the table for support, then to lift one foot up in back of him- or herself. Scan across the bottom of the shoe. Repeat for the other foot. The operator should expect to hear a short squeal from the detector when scanning the bottom of shoes or boots with steel shanks or steel toes. Both shoes should cause equivalent squeals.
  7. For the head area, start at the top of the forehead and scan around the top of the head down to the back of the neck.
- Given that the type of hand-held detector being used is the kind that provides different volumes of feedback, i.e., a soft squeal versus a much louder squeal, the operator will be able to distinguish between the detection of a smaller innocuous item or material, such as a zipper, and the detection of a larger, more suspicious item. It is important to be attuned to

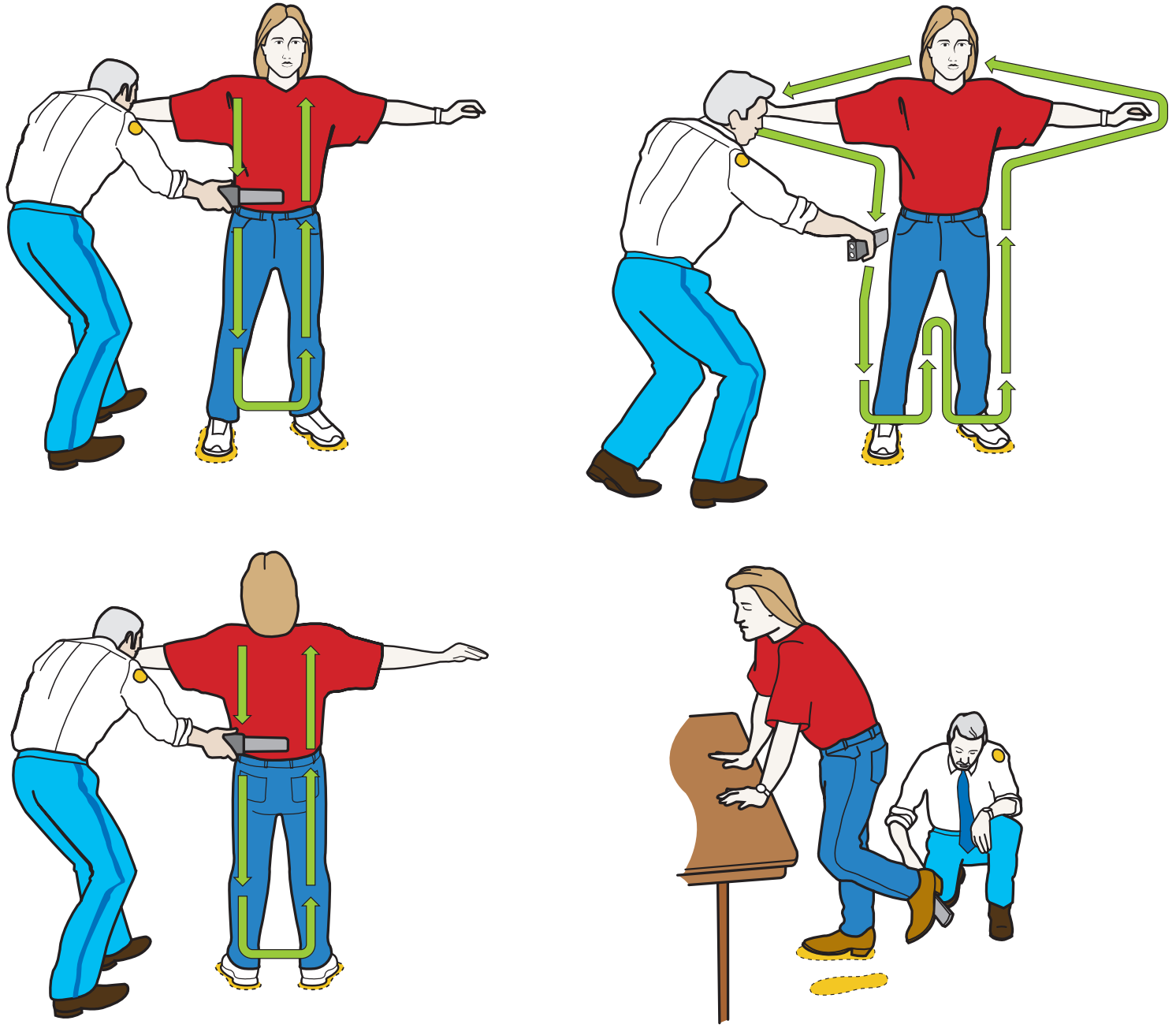


Exhibit 3.10. This is an example of procedures for using a hand-held metal detector that has at least a 10-inch zone of detection.

these different volumes to recognize when further investigation is required for a particular scannee.

- When the detector identifies a suspicious item and there is no visible source for the alarm (clothing is shielding the source object), ask the person to show you what they have in that area. For example, for an alarm along the arm or wrist, have the scannee pull up his or her shirt sleeve. Using your detector, duplicate the squeal you heard before, but now over the visible item.
- Do not let the scannee influence you as to what is actually causing an alarm (exhibit 3.11). For instance, if the detector denotes the presence of a suspicious item under a shirt sleeve, do not fail to completely investigate the source of the alarm even though the scannee assures you that it is just his or her watch.
- If the person you are about to scan caused an alarm when walking through a portal metal detector, and your job is to try to locate the source of that alarm on his or her body, do not stop the complete scanning process just because you come across one alarm-causing item. Continue the scan even though you find one or more items in the process.
- The lower abdominal area is particularly difficult to scan because this area is private in nature and because of the metal items usually found in this area: belt buckles, metal buttons or snaps, and metal zippers. When doing the initial front body scan, if an alarm occurs in this area, there are two possible ways to further investigate:
  a. Ask the scannee to undo any belt he or she might have on and have him or her pull the belt ends away from the middle of the body. Now scan the zipper area; the feedback volume from your hand-held metal detector should tell you if it is now only sensing a zipper and/or a metal snap, or if a more suspicious item is present and further investigation is needed.
  b. A second approach that some schools use is that, if the lower abdominal area is causing an alarm on the hand-held detector, ask the scannee to bend the front of his or her front waistband forward, to ascertain that no weapon is hidden behind it. Facilities need to be available for situations where further investigation can be accomplished privately, but only in the presence of two or more school employees who are the same gender as the scannee.

6. Instructions for the scannee

Education is important in enabling your scanning program to operate smoothly. Before the initiation of a weapon detection program, presentations and handouts should describe to the students, employees, and parents the items or materials that will make it more difficult to get through the scanning process quickly. If your school is also using x-ray technology for purses, bookbags, and so forth, consider asking students to put all alarm-causing items into their bags before they enter the scanning process.

For visitors and first-time scannees, it is very helpful (and will save time) to give them an idea of the process they are about to go through. Particularly helpful are posted instructions that are simple and quick to read, with diagrams showing what is expected of the scannee. An example of such instructions follows:

> Welcome to our school. For the safety of our students, employees, and visitors, our policies require that EVERY person be scanned and his or her carried items searched to prevent weapons from entering our school.

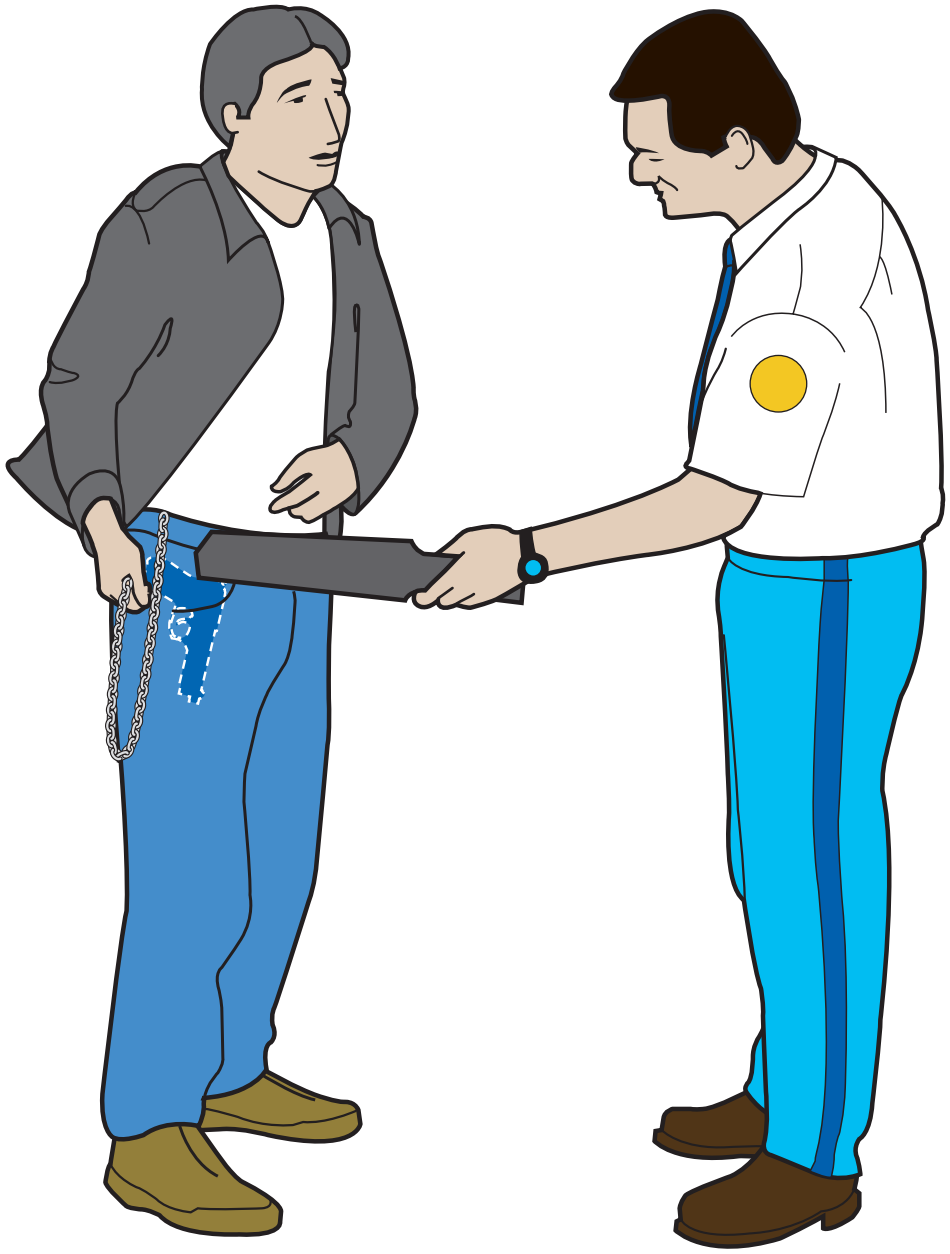


Exhibit 3.11. Here, the scannee is attempting to influence the operator by claiming that the chain is causing the alarm, when, in actuality, there is a hidden weapon.

When it is your turn, please stand first on the footprints on the floor. Extend your arms out to your sides, parallel to the floor.

If requested by the security personnel, please open your belt and extend both belt ends away from the front of the body.

To scan shoes, please grab the edge of the table and hold each foot, one at a time, out in back of you.

7. Maintenance and expected lifespan

If not accidentally or intentionally abused, most good hand-held metal detectors will require no maintenance. Extended maintenance contracts are usually not required beyond the initial warranty period. The only in-house maintenance that will be required is to provide for the recharging of batteries each night and/or making certain that new batteries are always available.

Most good hand-held metal detectors should have a useful lifespan of about 5 years, much more if used infrequently and possibly less if in constant use.

8. Working with the vendor

If a school is required to go out on bid for one or more hand-held metal detectors, it is recommended that the contract require the following optimal features:

- A variable pitch of alarms that provides more information to the operator using it, i.e., a softer squeal for an innocuous item, like a zipper, and a louder squeal for a bigger, more suspicious item.
- A detector paddle or zone that is at least 10 inches long.
- A signal that indicates the battery is beginning to run low, as opposed to an abrupt termination of operation.

C. X-ray baggage scanners

1. Safety concerns

X-ray equipment is available for the detection of weapons within baggage or other carried items. For single-energy units appropriate for school applications, a vacuum tube emits x-rays on and through these items. These x-rays come from inside the top of the unit and scan downward as baggage is automatically moved through the equipment. Sensors collect the magnitude of the signals that make it through scanned items, with low Z-number material allowing more energy through and material with high Z-numbers allowing less energy through. (A “Z number” is the atomic number of a particular element; a low Z in x-ray terms is any atomic number less than 26. A high Z in x-ray terms is any atomic number equal to or greater than 26.) The resulting images are transferred to a TV monitor, where an operator must carefully examine each image for evidence of firearms or knives.

The safety aspect of x-ray equipment for baggage inspection has improved greatly over the past two decades. This application of x-rays previously used a large cone of energy in order to make an image of an entire piece of baggage at one time. Today’s x-ray machines for baggage use a much lower energy pencil-thin beam of radiation that generally scans back-and-forth across a piece of baggage as the baggage moves beneath it. More sensitive sensors can now adequately capture an image with these lower dosage x-rays.

Infrared (IR) beams installed within the equipment can accurately start and stop the x-ray beam source so that the x-rays are not operational when there is not a piece of baggage located in imaging position. Add to these improvements the excellent shielding built into x-ray detectors, and it is easy to understand what has made modern baggage detectors quite safe and of negligible health risk to either the operator of the equipment or to the general public. Indeed, the radiation exposure to operators from baggage scanners has been shown to be only a few microrems per hour, which is equivalent to standing in the sunlight for a few minutes. Even smoking a cigarette gives a person a larger dose of radiation. About the only potential health risk from an x-ray baggage machine would be to someone attempting to ride the conveyor belt through the equipment, which would still result in substantially less radiation exposure than would be gained from a medical x-ray.

There have been concerns raised about the safety of exposing food to baggage x-ray machines. The U.S. Food and Drug Administration (FDA) has approved much higher doses of radiation for normal food preservation methods than any food items would receive going through x-ray baggage equipment. Most scientists feel that the FDA is quite conservative in the limits it has established.

Over the past 10–15 years, x-ray detectors have become quite safe for camera film because of lower dose x rays. This would include the x-ray equipment most schools would normally consider purchasing today but not, perhaps, an older piece of equipment that has been donated for the school's use. One modern exception to this is the much more sophisticated $1million x-ray machines that are used on some airline flights to examine checked baggage. This equipment is used to search checked baggage for explosives, and it may well damage camera film.

2. Setup and space requirements

A typical x-ray baggage scanner will have a footprint about 4 by 4 feet in size. This does not include any type of conveyor belt to automatically move items into and out of the x-ray imaging area. The smallest conveyor belt that would probably be useful for a school application is 8 feet in length, which would add about 2 feet on either side of the detector itself. Conveyors can come in almost any size; typical conveyors for airports are a total of 10–12 feet in length.

Smaller desktop x-ray units are available but are used primarily for screening letters and mailed parcels.

Unlike portal metal detectors used for personnel, x-ray baggage scanners are not sensitive to their surroundings. Virtually no clearance is needed around the equipment except for space for on operator to sit or stand at the controls, which are located to the side of the unit.

A school should have the factory or vendor install, set up, and calibrate the x-ray detector. After installation, moving the equipment to a different onsite location is generally not a problem. While the equipment should not be abused, it is not overly delicate.

3. Throughput

The expected throughput of an x-ray baggage scanner will depend on two things: the efficiency of the operator and the amount of clutter in a typical bag at this particular school. Clutter can also affect the speed

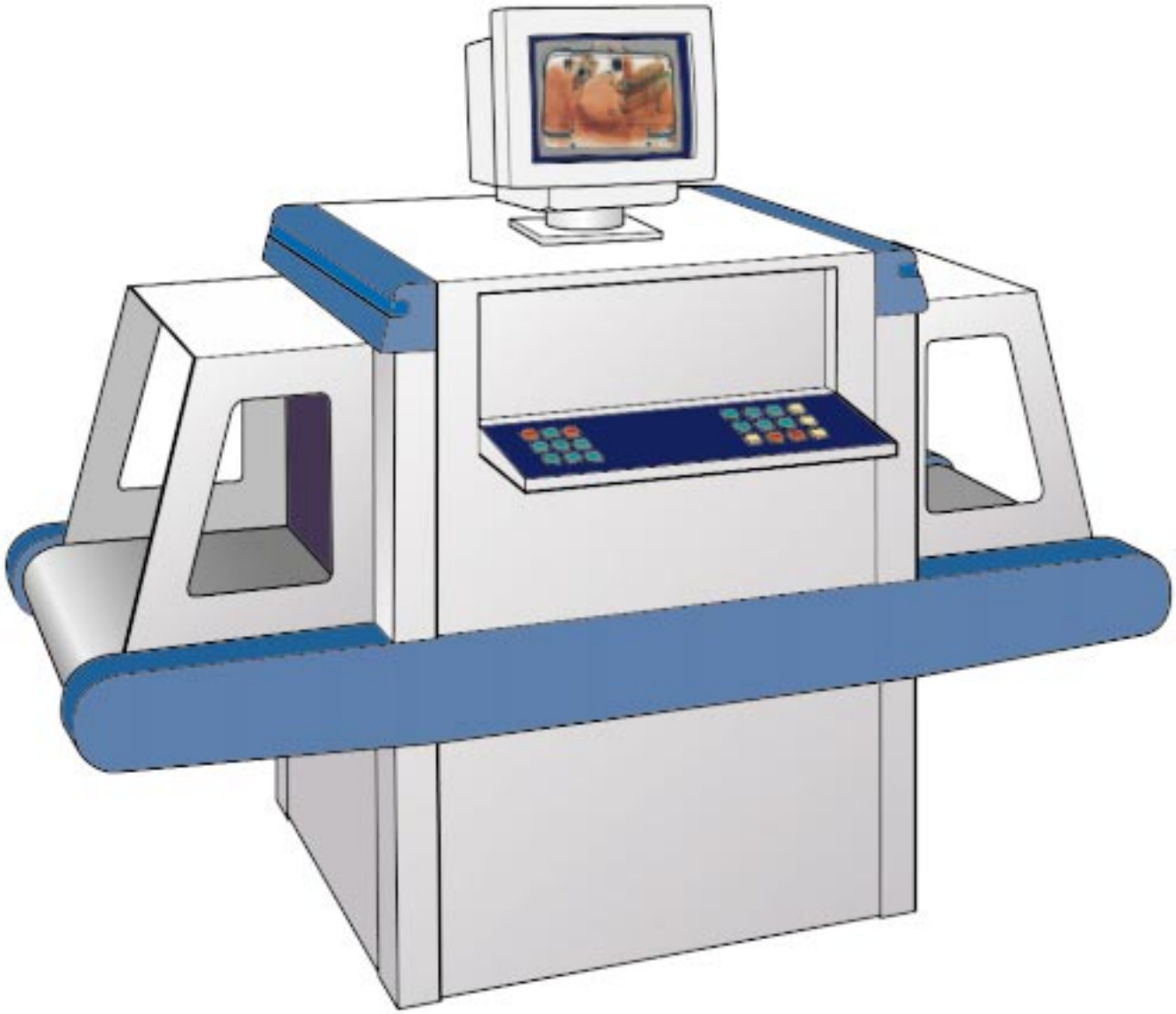


Exhibit 3.12. An illustration of an x-ray baggage detector.

of the operator. Carried purses and bookbags that contain many high Z-material items, such as metal rulers, screwdrivers or other tools, metal aspirin tins, foil-wrapped items, and so forth, can significantly slow down an operator who is examining each piece of baggage. Fortunately (or unfortunately), in most schools where the security equipment operators become familiar with the individual students and the kinds of things they usually carry, the speed of an operator will increase.

Generally, between 10 and 20 items per minute can be examined using an x-ray baggage scanner. As many as 30 items per minute can be effectively scanned if most of the items are benign, i.e., contain no obvious metal items larger than a coin or button, none of which are touching in the image. Dense clutter within a bag will necessitate that bag being pulled off the conveyor to be manually searched.

4. Hardware costs and manpower costs

X-ray detectors for baggage are not cheap. Most appropriate for schools is a single-energy unit (one radiation source) costing about $30,000. There are much more expensive models on the market, ranging from $250,000 to $1 million, but these are used in applications concerned more with the detection of explosives. The detection of drugs is also possible, but the sophisticated equipment needed is too expensive for most schools. Schools will generally use a black-and-white monitor with the x-ray machine. Some models add the convenience of a color monitor, which may not add any valuable information to be used in decision making by the operator. Again, costs limit most schools to black-and-white monitors.

The conveyor belt needed to feed items into and out of the x-ray detector will generally be priced as part of the total system cost.

The manpower cost for operating this equipment is very high. For low-volume applications, in which baggage comes through slower than one bag per minute, one full-time operator will be sufficient to help with the placement of bags on the conveyor belt, operate the controls, view the monitor, make a judgment regarding each bag, and perform any needed manual searches. However, it is generally recommended that one operator work at the monitor of an x-ray machine no more than 2 hours at a time and preferably no longer than one-half hour at a time, trading tasks with another security person.

Most high-volume facilities, including airports and schools, will have two operators assigned to each x-ray detector. In this way, the operators can switch off the task of watching the monitor and of performing manual baggage searches as required. Airports will normally give these operators a break every 2 hours because of the intensity of the work, but most schools will not be engaged with intensive baggage scanning for more than 2 hours.

For schools, it is not the length of time an operator has to work that is of concern; rather, the issue is the number of operators needed during a relatively short period of time and the number of x-ray units required to maintain an adequate throughput during the morning rush. While it is probably a simple matter to hire one security aide to work 8 hours a day, it is much more difficult to find eight security aides to work 1 hour a day. (Eight or more security personnel would normally be required to support the equipment and

processes in a complete weapon-detection program at a school with 2,000 students.) For this reason, it is not unusual for a school administration to use fellow administrators, teachers, and other employees to supplement the security personnel running the equipment each schoolday morning. Employees may be pleased to earn the extra money, but the administration must be certain that all receive adequate training.

Who will run the equipment the other 7 hours of the schoolday? This can be expensive and a somewhat low payback effort. An approach implemented by some schools is to enforce a policy that the school doors are basically locked one-half hour after school begins in the morning. Although this is a rather harsh stance, it may be necessary in a school where resources are limited but the threat of weapons is quite high.

Vendors will normally provide initial training at no additional expense. A 4-hour course will adequately introduce a new operator to the overall use and safety information of an x-ray detector, but practice and experience is equally important. Interesting training aids are currently available from some vendors. Prepared images of baggage going through the x-ray scanner can be played back on the TV monitor for operator practice. Another feature on some equipment will randomly superimpose the image of a suspicious (but fictitious) item over the actual images being captured during the normal work time. These phantom images may help operators to stay aware so that they are not lulled into complacency by the routine absence (hopefully) of any weapons coming into a facility.

5. Procedures for the operator

The actual operation of an x-ray baggage scanner is straightforward. Vendors will provide recommended procedures for operating their specific equipment, and each school will probably tailor this for its own environment. However, as with the radiologist who examines medical x-rays, the challenging part of operating x-ray equipment for weapon detection is knowing what to look for. The untrained or disinterested operator can negate any possible benefit that could be gained in a weapon detection program.

The TV monitor that displays the black-and-white x-ray images of baggage it is scanning can usually be used in the positive or negative, i.e., solid objects can be displayed as light or dark objects. There are two types of color systems on the market. There are colorized single-energy (one radiation source) systems in which the color is arbitrarily assigned based on the level of energy transmitted. The second type is a dual-energy (two radiation sources) system that assigns color based on the effective Z-number of the material. The first type is inexpensive but adds no useful information to the display. The second type adds useful information but would normally be cost-prohibitive for most schools (exhibit 3.13).

Some general guidelines for the operator of an x-ray detector are:

- The different models of x-ray detectors utilize various techniques and angles for transmitting the radiation and receiving it on its sensors. Your vendor will inform you as to the best orientation for items being scanned by your equipment. For example, for an x-ray detector that uses a fan-shaped beam emanating from the top of the equipment's interior in a downward direction, the vendor will give instructions similar to:
  Do not put a bag down on a conveyer belt such that

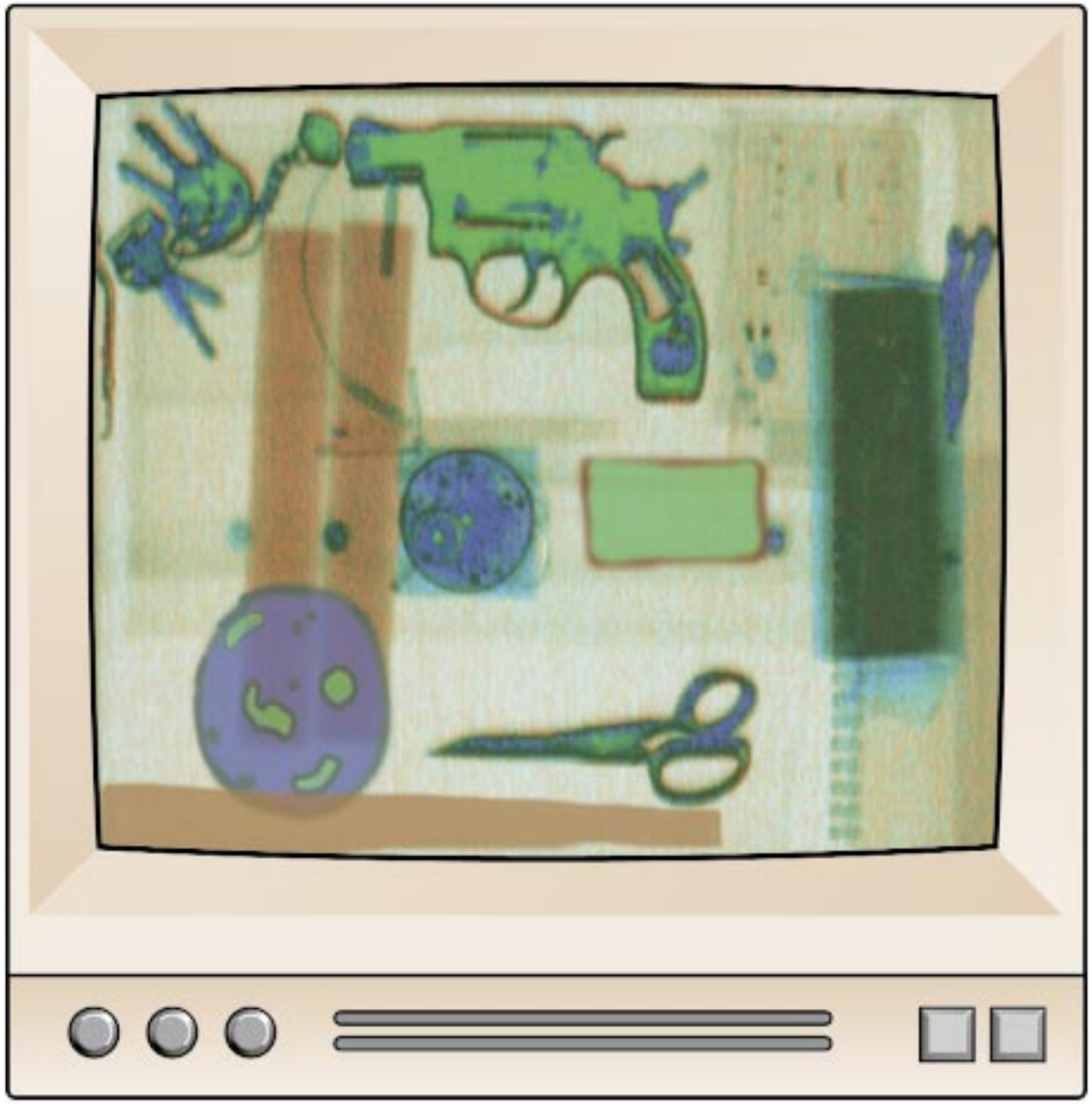


Exhibit 3.13. An example of a dual-energy x-ray machine that assigns color based on the effective *z*-number of the material. This is an informative system but normally too expensive for schools.

the images captured will be of the narrowest perspective of the bag. Lay the bag down on its widest side to allow the x rays to penetrate the least amount of material. Be careful that no part of the bag is outside the zone of detection, which is generally defined by the width of the conveyor belt that is used.

- What you are looking for is a solid dark object (if display is set this way) that could be a weapon, part of a weapon, or hiding a weapon. A best case scenario (for the operator) is a revolver that is lying on its side so that its shape is obvious. The same is true for a knife of substantial size if it is lying on its flat side. What becomes difficult, and where most operator training and judgment come into play, is when a weapon is in a different orientation so that it is viewed from the top, bottom, or back of the weapon. A revolver will generally still have a revolver shape that reveals its cartridge. An automatic weapon viewed from the top, however, will produce an image that is an innocuous rectangle 4 inches or more in length. (Keep in mind that there are some weapons available today such that the length is less than 3 inches.) An automatic or semiautomatic weapon viewed from the back is an even smaller rectangle. And, unfortunately, a knife can be very difficult to detect if it is made of any material other than metal.
- Clutter occurs where several dark items are grouped together in an x-ray image, such that the actual size and shape of each item cannot be reasonably determined. More often than not, clutter is the cause of manual searches in weapon detection programs.
- Surprisingly, band instruments can usually be put through an x-ray machine successfully; the normal thinness of the metal of most instruments will allow the x-ray detector to see within and behind the instrument for any hidden weapon. The school should screen all of the different types of instruments beforehand to determine if any of the instruments (or their cases) will be a problem for the x-ray detector.
- When in doubt about an object in a bag, investigate!

6. Instructions for the scannee

Hopefully, as students grow accustomed to what items in their bags and purses trigger an alert to the operator of the x-ray equipment, they will tend not to bring these items to school with them. This may not be the case for disruptive students, who may go out of their way to slow down the system. School administrators may want to consider having some type of consequences in place if this behavior continues.

Educating students and parents in advance about what to expect from the x-ray process and which of the items they carry will result in bag searches can help speed up the process at the beginning of a scanning program. However, do *not* share with the students information regarding the system's weaknesses and what makes it difficult to recognize weapons hidden inside bags. This information should remain restricted to appropriate school and law enforcement personnel responsible for security.

A simple set of instructions located at the x-ray detector can remind students quickly of what is expected of them. An example of such a sign is:

> Place all large jewelry, watches, belts with metal buckles, large keyrings, loose change, and other detector-sensitive items in your backpack or purse. (This first sentence is for a school that also has portal metal detectors.)

> Lay all books, notebooks, purses, bags, lunches, backpacks, briefcases, hats, coats, jackets, and electronic devices on their widest side on the conveyor belt. (Adjust according to whatever orientation is best for your equipment.)
>
> Do not stack items; place them on the conveyor belt separately. It is easy to reduce the chance of security personnel going through your things manually—DO NOT CARRY A LOT OF JUNK IN THEM!

There should be a sign on the other side of the x-ray detector:

> Please immediately check for all of your personal valuables and possessions. The school is not responsible for your things. If you have irreplaceable items, please do not bring them to school.

7. Acceptance testing and performance testing

The American Society for Testing Material (ASTM) has defined a test procedure that most schools will want to use as part of the initial acceptance test and also incorporate into their regular performance testing. This test uses a 10-step wedge of milled aluminum (exhibit 3.14). Across the bottom of the step wedge are several wavy wires of different gauges. The x-ray detector is performing well if, when this step wedge is sent through the detector, 10 different shades of gray are clearly distinguishable and a certain number of the wires are also seen. (A very good x-ray detector will see even the smallest gauge of wire behind the thickest step of the step wedge.) This step wedge will be available through your vendor, who will likely employ the same tool for its own testing purposes.

Schools should initially run this test to accept the equipment and on a regular basis, such as once a month, for validating that the system is still performing well. Any significant decrease in the number of wavy wires that are visible may indicate that the unit needs repair.

8. Maintenance and expected lifespan

Most companies offer extended warranties or maintenance contracts for x-ray baggage scanners. Service contracts are generally more expensive than what you can expect to spend over the life of the equipment for repair. However, depending on the fiscal arrangements at each facility, some schools may want to establish a service contract up front, when they have the funding available. (Schools can never be certain what their budget will be in subsequent years, and coming up with $5,000 for a repair bill 3 years from now may not be possible.) In the absence of such a contract, schools should contact the factory when repair is needed.

Most x-ray baggage scanners will have a life of 10 years or more. Technology advancements are more likely than failure to render them less useful. Over the course of this time, there is a reasonable chance that a facility will need to replace the vacuum tube that is the source of the x rays.

There is little regular maintenance required for this equipment. The largest moving part, the conveyor belt, often is self-oiling, and the facility may only need to add oil to a reservoir occasionally. Individual vendors

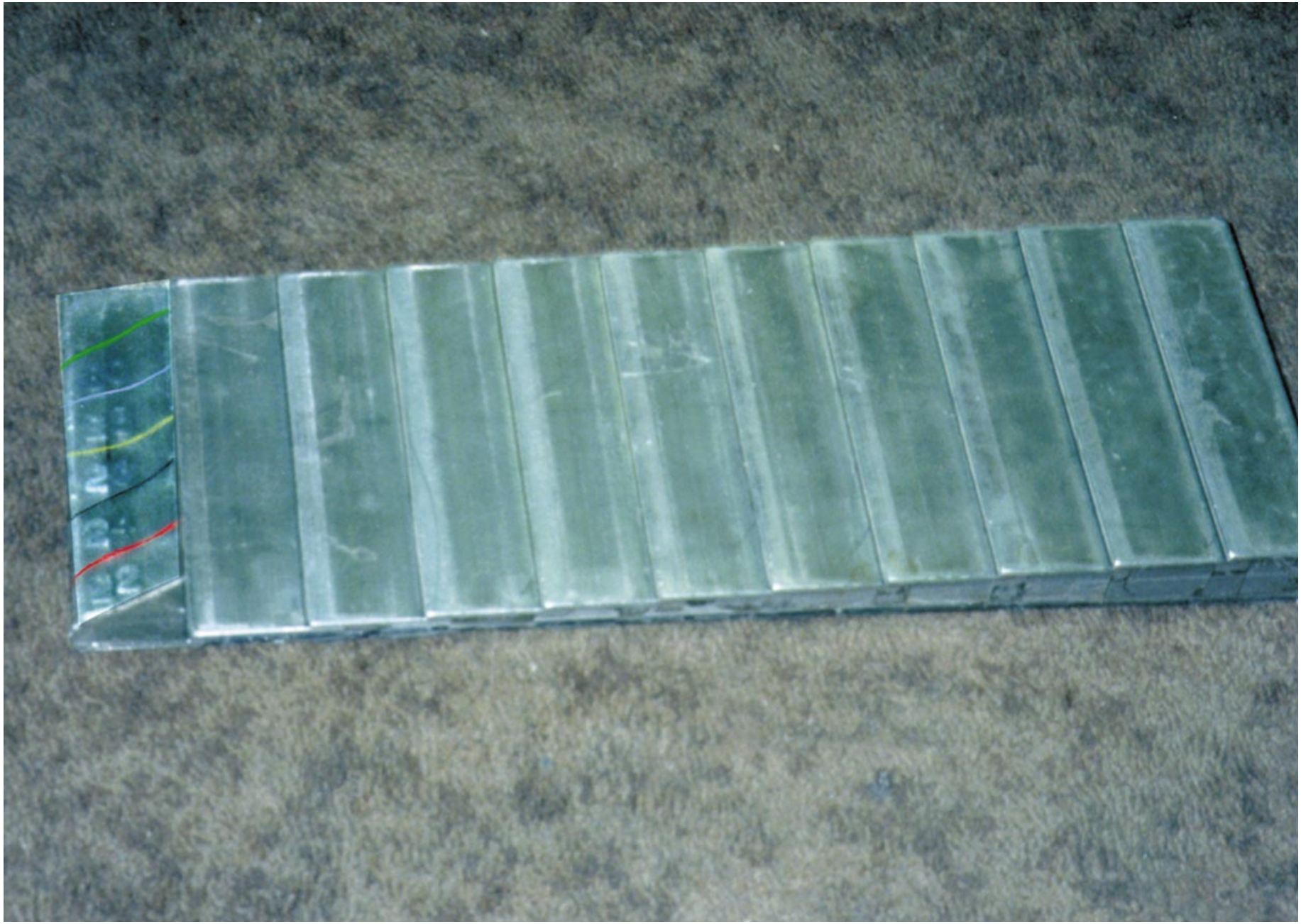


Exhibit 3.14. This 10-step wedge is used for x-ray baggage scanner acceptance testing and regular performance testing.

may recommend certain procedures be run periodically (once a month or so) to test for radiation leakage, even though the chance of such leakage in modern x-ray detectors is small. Heavy damage, malicious acts, or purposely holding the shielding flaps aside while the machine is in operation would normally be required to allow radiation leakage.

9. Working with the vendor

There are several excellent products on the market that would be appropriate for use by schools. A school security person or administrator should take the time to visit one of the national trade shows where most of this equipment is on display. Seeing the equipment and talking with vendors can often help a facility gain a better understanding of the products that they are considering using. Such a visit allows schools to identify the vendors they would like to seriously consider.

Because of the high cost of this equipment, schools may want to invite at least two different vendors to visit their campuses and demonstrate their equipment. This is not a trivial expense for a vendor and should not be done unless a particular product is actually under consideration. When equipment is available for testing on campus, the security personnel can become familiar with the operation of the equipment and what options might be appropriate for their school's needs. If at all possible, a school should involve the people who are going to run the equipment in the decisionmaking process.

Given that all the available x-ray baggage scanners are priced similarly, operate easily, offer substantial training up front, and have good quality monitor images, schools will be most concerned about service. If a service contract is being purchased, it may be possible to include language in the RFQ requiring the chosen vendor to provide service and repair within 3–5 work days or to substitute a backup system within 48 hours. This may be easy to incorporate within a large city but impossible in more rural locations. If a particular school district is planning on purchasing several units for multiple schools, the district may be able to negotiate an excellent price that will include one backup unit that will be stored by the vendor for use when needed. This backup unit may be a used product that is in good working order and easy to bring in quickly and set up during a crisis.

Chapter IV Entry-Control Technologies

Many school administrators contend that the majority of the security problems and incidents at their schools are the result of an unauthorized person being on campus (albeit the vast majority of these unauthorized persons are in some way related to the school or to students at the school). These trespassers can include a school's own suspended or expelled students, students from rival schools, irate parents seeking revenge against a student or employee, gang members, or even drug dealers. It is logical, then, that if a school were able to carefully control exactly who was able to enter the campus or school buildings, security incidents would drop significantly. This is easier said than done.

Schools can often prevent or discourage the casual intruder. Some of the less technical, though often quite effective, approaches to deterring unauthorized entry are:

- Posted signs warning that unauthorized trespassers are subject to arrest.
- Signs that inform visitors that all vehicles brought onto campus are subject to search by the school.
- A guard who is checking identifications at the main entrance gate to the campus.
- Vehicle parking stickers so that any vehicle found parked on campus without a sticker, other than in the monitored visitor lot, is subject to being ticketed and towed.
- Uniforms for students, which make outsiders very identifiable.
- A school policy of no hats; no droopy pants; no t-shirts with alcohol, drug, violence, or gang affiliation messages; or no exposed tattoos, which again can help make outsiders identifiable.
- Greeters at all open entrances to school (these can be parent volunteers).
- Minimal numbers of entrances to the campus and to the school. Superfluous exterior doors should be locked to prevent entry from the outside and labeled inside: "For emergency exit only—alarm will sound."
- A policy that anyone walking around campus during classtime will be challenged for a pass and/or student ID and is subject to being searched or even scanned by a metal detector to be checked for weapons and/or drugs.
- The main student parking lot (which does not include parking for work-study students) closed off and locked during the day. Make entry to school during the schoolday possible only through the front office.
- Fencing around campus that will discourage the casual intruder and better define school property.
- A policy that, when a student is expelled or suspended, his or her student ID is confiscated and (for a larger school) his or her picture is made available to the security staff.

A. Limiting entry/exit points

Most U.S. school buildings in use today were originally designed to foster learning, mimicking universities to some extent. Often, their layouts provided many secluded niches to allow students privacy in which to study; separate buildings to house the various disciplines; multiple entrances and exits in buildings to maximize fire safety and emphasize freedom; and spread-out campuses to prevent congestion and to be open to the community. Fences became passe, perhaps for appearance but more likely to cut expenses. Some schools even have public streets running through the campus. These designs were very appropriate and greatly enjoyed 30–40 years ago. Entry control in these facilities has been limited in the past to the coincidence of an adult noticing an outsider on campus and challenging that outsider.

For current security needs, controlling the access of students, employees, and visitors has become paramount. Without major remodeling for some schools, the manpower required to accomplish access control could be enormous, both for entry into buildings and onto the campus itself. (One fairly new high school in Colorado consists of 1 large building but has more than 100 exterior doors.) Technologies such as card swipes or keypads can greatly reduce this manpower requirement, but not without significant expense.

To best control a school building and/or campus, the number of entryways into the building or onto the campus must be severely limited. Just as with any high-security facility, restricting normal entrance to only one or two locations can greatly reduce the number of security personnel or security devices that must be supported. But limiting entry points can be very difficult for some schools, due to building layout, required emergency egress, property boundaries, the surrounding neighborhood, and adjacent streets.

Some urban schools have no campus per se; their buildings sit directly on streets on one or more sides. This can somewhat reduce the entry control problem but has some inherent problems of its own.

For those schools with campuses, fencing is usually important to control entry onto the school grounds. It is important that schools and communities recognize that enclosing a campus with fencing is more to keep outsiders out than to keep insiders in, although its presence does tend to reduce truancy during the schoolday. Controlling campus entry requires fencing or other physical barriers.

Fencing does not have to be unattractive. Razor tape or barbed wire is rarely appropriate for a school setting but may sometimes be necessary due to vandalism or theft at a school. If adequate funding is available, wrought iron fencing can enhance the appearance of some campuses, while providing a very difficult barrier to climb over. Less expensive but still providing an excellent barrier is an 8-foot chain link fence (exhibit 4.1) with small mesh (1-inch to 1½-inch). Unlike a typical 6-foot chain link fence, it is difficult to pull up on an 8-foot high fence and a smaller mesh will not allow toeholds. This more desirable 8-foot fencing material is usually about twice the cost per running foot as the cost of standard 6-foot fencing material, but it is probably worth the extra cost, depending on the particular school's risks.

A robust fence defines property boundaries and forces a perpetrator to consciously trespass rather than allowing idle wandering onto a campus that has no fencing. The goal of fencing is to deter the casual or unmotivated trespasser. No fence can keep out someone determined to enter the campus who comes prepared or who is very motivated (i.e., brings a ladder or wire clippers, smashes through the fence with a vehicle, and so forth).

Fencing may be less important for a school that is located in a somewhat remote location. If the majority of students, faculty, and visitors must necessarily get to a particular school on buses or in cars, then the act of restricting vehicle entry to one or two driveways and posting a guard at these locations to validate all vehicle occupants may be adequate without the enclosure of fencing.

For campuses where entry into the building(s) is controlled/restricted and students do not congregate outside during the day, again, fencing may be less useful.

Exhibit 4.1. This 8-foot, small-mesh fence is around an elementary school. The school's problem with outside gang confrontations on the playground was completely eliminated.

B. Entry-control approaches

Once entrances to a facility are limited in number, the process of allowing or denying access is generally accomplished through one of four approaches. The first and most common approach is manpower intensive, and the remaining three employ technology devices. The level of actual security achieved is generally believed to be from 1 to 4, lowest security to highest security, but this is subject to many other variables. These four approaches are:

1. A security guard controls entry; ID cards or other means of identification may be checked. (WHO lets you in)
2. A special ID card/badge with automatic readers. (What you HAVE)
3. A PIN number for entering on a keypad. (What you KNOW)
4. A biometric device for feature recognition. (Who you ARE)

The following sections provide further details. The second, third, and fourth approaches utilize technology, as illustrated in exhibit 4.2.

1. **WHO lets you in.** A security person (or a person assigned to this duty) is located at some particular entry point, either at the vehicle entrance onto campus or at the main entry doors into the building. This security person establishes that the person wishing to enter is a valid student, employee, or visitor. In smaller schools, this can often be accomplished with no more than the recognition of the person by the security person. In larger schools, this validation can be accomplished through issued ID cards (usually with photos), badges, vehicle stickers, or mandatory school uniforms. Although this is not considered a high-security approach for the reasons listed below, it can be one of the most expensive approaches for most schools.
   - Strengths: A security person can do more than simply check an ID card. He or she may also notice if something appears amiss, such as if a student is drunk or acting strangely. A security person can also prevent two or more students from entering using one ID card.
   - Weaknesses: A security person in this task can become bored and may become careless or move to a different job. A security person's attention can be diverted. A dishonest security person could allow unauthorized individuals to enter. Using a person for entry control is an ongoing expense for the school. A simple picture ID card can be stolen and used by someone else; experience has shown that security personnel can sometimes fail to identify persons who have an ID card with someone else's picture.
   - Costs: Depending on the part of the country, each security guard will cost between $8,000 and $30,000 per year, plus training, uniforms, and so forth. (This does not apply to the costs of an actual law enforcement officer.) One guard can be expected to handle roughly 250–350 cars per hour, providing that vehicle occupants are prepared to show ID immediately.
   - Every member of a school's security organization must have a thorough background check before being hired, with references and previous employers called. If possible, periodically require drug testing on a random basis.
2. **What you HAVE.** In this approach, an ID card or badge is specially encoded to be recognized by a card reader. Validation of the card can be designed to electronically open a door lock, allow a turnstile

Exhibit 4.2. These are three technology approaches to entry control.

to operate, or lift a mechanical arm that extends across a vehicle driveway. Viable card technologies for schools include bar codes or magnetic strips for card-swipe readers (such as those used for most credit cards) or passive or active radio frequency (RF) cards for proximity readers, which can validate a card several inches to several feet away (depending on the cost of the system). Card-swipe readers are probably more subject to vandalism as their read heads are fairly delicate. Proximity readers can be protected with a solid piece of plexiglass because actual contact of the card is not required. A proximity card reader might be an ideal entry control system for a teacher's parking lot, or for a computer lab. The newer smart cards are probably overkill for an entry control system.

- Strengths: No manpower is involved. These are mature technologies. Validation of a card can be turned off if the card is lost or stolen. When used in conjunction with a floor-to-ceiling turnstile, an authorized person cannot bring in unauthorized persons (exhibit 4.3). It is also possible to automatically update an attendance database when an ID card is read. These cards are generally tamperproof, and some have features that make them very difficult to counterfeit.
- Weaknesses: For an electronic lock or vehicle barrier, there is no way to ascertain that only a single authorized person is entering. Cards can be lent out. Cards can be used by others until the card is turned off by the school administration. Card-swipe readers can be subject to vandalism if in a vulnerable location. Card readers require a certain level of overhead to maintain, and regular updating of their databases is mandatory.
- Costs: Prices for the equipment to produce high-quality, tamperproof ID cards, with software to develop attractive customized designs, have come down greatly in just the past few years. A sophisticated printer that embeds the ink into the card cost as much as $25,000 just 4 years ago. Today, an entire system (a printer, a digital camera, and the software to operate them) that is more than adequate for most school's needs can be purchased for $6,000–$8,000. While every product is different, and there are many features that can be added that raise the price considerably, the supplies (inks, card blanks, and so forth) that a school must continually purchase to create cards readable by a card-swipe reader will cost the school about $1 per card. Supplies for cards readable by a proximity reader will run between $3 and $10 per card, depending on the capabilities of the system. Card-swipe readers and proximity readers cost between $150 and $300 per reader. The electronics, field panel, and computer system necessary to support a modest number of readers (typically, eight or fewer) will cost around $2,000–$3,000. Installation is usually a job most appropriate for an electrician.

3. **What you KNOW.** A personal identification number (PIN) or special code is entered on a keypad. This is usually used in conjunction with an ID card and card reader. Alone, a PIN used on a keypad could be easily compromised by an onlooker; if used in conjunction with a card reader, the level of security is substantially higher. Sophistication of keypads runs from very simple entry devices to unique scramble keypads that effectively allow only the user to view the numbers and that scramble the numbers differently for each use.

Exhibit 4.3. These turnstiles operate when a valid ID card is scanned through the card-swipe device; this type of arrangement can prohibit more than one person from entering with one valid card.

- Strengths: The PIN and ID card can be turned off when no longer appropriate. A stolen ID card is not enough for a trespasser to use for entry. It is also possible to automatically update an attendance database when an ID card is read and the PIN entered.
- Weaknesses: More administrative effort is required to maintain a card system and keypad system. Except when used with a floor-to-ceiling turnstile, it is possible for an authorized person to allow unauthorized persons entry. Users can forget their PINs. Users can lend out their PINs and cards. Keypads are vulnerable to mechanical malfunction as well as vandalism.
- Costs: Simple stand-alone keypads, hooked directly to an electric door latch, lock, or strike, may cost less than $200 for all the necessary hardware. However, installation may be difficult on an existing door. More sophisticated keypad systems that may be part of a network of keypads can cost from $1,200 to several thousand dollars.
- An ideal application for a keypad system is for a relatively small population size that does not change often. (For example, the chemistry storage room that only the chemistry teachers have a code to enter.) For these applications, where the keypad is not subjected to abuse or a harsh environment, a keypad system can go for many years without any additional maintenance or adjustment.

4. **Who you ARE.** An electronic device verifies the identity of a person through the use of a personal attribute, such as hand or finger shape, fingerprint, voiceprint, signature dynamics, retinal pattern, or iris pattern (exhibit 4.4). These devices, known as biometric identifiers, can be very accurate. The chances of such devices mistakenly allowing an unauthorized person into a facility is usually much lower than the chances of a guard inaccurately matching faces to picture badges. Biometrics are commonly used in high-security applications where unauthorized access into a facility is unacceptable. Recently, two elementary schools in New Mexico have been using hand geometry systems to verify custodial parents, as the abduction of a child by a noncustodial parent is one of their greatest vulnerabilities.
   - Strengths: This form of identification cannot be lent to other people. A particular person's identification can be deleted from the database when no longer appropriate. There is nothing for a user to forget to bring with him or her. Hand or finger geometry appear to be viable, affordable, and user friendly biometric devices for medium- or low-security applications. Retina or iris pattern scanners are probably the most accurate of all biometric devices, and are most appropriate for high-security facilities. Voice recognition systems have improved significantly over the past few years but still have some weaknesses to overcome before their use is widespread.
   - Weaknesses: Not all biometric devices are user friendly. Some devices are very difficult for certain individuals to use. Except when used with a floor-to-ceiling turnstile, it is possible for an authorized person to let in unauthorized persons. Some of these technologies are not completely mature, in that their occasional tendency to falsely reject an authorized person can be unacceptable in a school environment. The devices are subject to damage from vandalism. It usually takes longer to use a biometric device than a card reader or keypad.

Exhibit 4.4. Illustrated here are several types of biometric identifiers that can be used for entry control with a high confidence of accuracy.

- Costs: These technologies continue to improve, and new biometric devices are always being brought to market. Prices for most of these devices have stabilized over the past 5 years. A stand-alone biometric unit can run between $1,200 and $5,000. A system that oversees and monitors biometric units at several doors can cost between $10,000 and $50,000.

Working with the vendor. Identification cards that are readable by an electronic device are probably the more viable technology for schools to consider for entry control. Dozens of different manufacturers are offering hundreds of devices that produce a wide variety of card styles and features. Visiting one of the security trade shows, such as the American Society of Industrial Security (ASIS) conference held each year, will familiarize an individual with most of the products available on the market. Some good questions to ask the vendor are:

- What is the cost of the basic printer, basic digital camera, and basic software? What additional features are available for each of these, how much are they, and what do these upgrades provide?
- What kind of computer will be required to run the system and with what memory and storage capabilities? What is the general speed of data input and card production that can be expected? What can be done (e.g., upgraded components) to speed this up? (An acceptable system may take between 1 and 2 minutes to produce one ID card.)
- Does the printer create both sides of the cards at once, or does the card have to be manually flipped?
- Will the vendor come and install the system and get it working initially?
- Will the vendor program the software initially for the first card design?
- What is the bulk cost of all of the supplies that will be needed? Is it reasonable to buy enough supplies for the next several years, or do some of the materials have a limited shelf life? How long are these particular supplies expected to be available?
- What maintenance is required on the printer and how often (i.e., after how many cards?)
- How long does it take to turn the system on before it is prepared to accept data for the first card?
- Is there any limit on the number of cards that can queue up waiting for the printer at any one time?
- What additional security options are available for the cards? (For example, some vendors offer hologram overlays, which may add $0.25 to the price of each card.)
- What are the names and phone numbers of schools in your State that are already using this device? How long have they had their systems?
- Did the other schools using this system find it difficult to use the system? Is training simple? Have they had any equipment breakdowns yet? Did any of the supplies not produce the number of cards they said it would? How many additional blank cards should be purchased for errors, redos,and so forth?
- How much space is necessary to set up the equipment and allow enough room for operators and waiting students?
- What happens if the system breaks in the middle of the registration of students?

Chapter V Duress Alarm Devices and Their Role in Crisis Management

It would be very unusual for a school to never experience a crisis situation. A crisis can be any incident whereby the health or well-being of one or more students or one or more employees is in imminent danger, or part or all of the school facility will potentially be destroyed or made unavailable. A list of crises could include:

- A threatening or drunk student or employee.
- A trespasser on campus.
- A fight.
- The breakout of a contagious disease.
- An irate and threatening parent on campus.
- Sudden unavailability of a teacher or a bus driver.
- A weapon known to be on campus.
- Massive vandalism.
- A utility outage (no water, electricity, heating, cooling, or telephone service).
- Bad weather (weather too bad to allow students to return home via normal methods or at normal times).
- A vehicular accident with injuries, either in or near the school parking lot or during a school-sponsored event.
- An extremely ill student or employee.
- A gas main leak or toxic spill on or near campus.
- A bomb threat.
- A gang confrontation on or near school property.
- A suicide.
- A hostage situation.
- A shooting, stabbing, murder, or rape.
- A bomb detonation inside the school facility or adjacent to school facilities (a car bomb).
- A local or National emergency that sends community residents to seek temporary shelter at the school.

For a school, a crisis that requires immediate response can be as harmless (but inconvenient) as the lack of a key to open the gym for an evening sporting event. Unfortunately, recent tragedies in the United States have demonstrated the need for schools to be prepared to respond to emergencies as serious as shootings or bombs.

How a school responds to this wide range of incidents is in itself an entire discipline—that of crisis management and planning. Every school needs a well-thought-out, annually updated crisis plan, with regular training for all those who might be involved. Not all schools have a plan, and many plans in existence were issued by the school district such that, by virtue of their generic nature, they may be inadequate for a true emergency. This plan needs to make assignments of who is in charge during different types of emergencies; who is the alternate in charge; who is called first, by whom, from where, and using what; whether students are relocated and how; how students are provided food, water, or shelter in the interim; what type of statement is made to the press and by whom; and who is in charge when emergency teams (fire, police, and so forth) arrive on the scene. These are only a few of the specifications called for. In the best of all possible situations, a predetermined team of school employees will immediately muster upon occurrence of a serious situation. Team members would know who to look to for decisions and then proceed automatically in their roles for the particular plan chosen to be implemented.

For the sake of this discussion, it will be assumed that a school has a current crisis plan in place. The issue that will be of concern here is how an employee (or student) can notify security, school personnel, and/or local emergency services that a crisis is occurring or is

imminent. Types of communication that may be viable are yelling/screaming, sending someone else for help, using the public address (PA) system, using a telephone, or calling on a two-way radio. (Two-way radios will be a selected technology topic in a subsequent manual.)

Now consider that the person who needs to summon help is in a situation where these options are not viable. This situation may be constrained by the need for extreme urgency or discretion (because of an intimidating situation) or because of the vulnerable location of the person summoning help. The provision that allows a person to summon help under one or more of these constraints is defined as a "duress alarm."

Modern duress alarms are generally electronic devices that vary widely in capabilities and price. There are three general overlapping categories of duress alarms that can send one or more levels of distress signals to a particular location:

- A panic-button alarm—a pushbutton mounted in a fixed location.
- An identification alarm—a portable device that identifies the owner of the device.
- An identification/location alarm—a portable device that identifies, locates, and tracks the person who activated the duress alarm.

(One additional category could possibly be the cellular telephone. While this approach is neither as discrete nor as automatic as the other three categories of alarm devices, a cellular telephone is highly recommended equipment for every principal and the primary security person. Land lines for telephone service are occasionally unavailable, whether due to inclement weather, accidents, or through malicious actions.)

The panic button is by far the most common type of duress alarm presently found in schools (exhibit 5.1). The simplest application would be a strategically located button that, when initiated, would engage a dedicated phone line. A prerecorded message specifying the school, its location, and the urgency is sent to several locations, such as the police department, the district security office, and so forth. Such a system could be pulled together for a few hundred dollars by the local handyman, plus the ongoing cost of the phone line.

Commercially available duress panic button systems provide a pushbutton mounted on classroom walls or under teachers' desks. In a duress situation, a teacher or other employee depresses the panic button, which transmits a signal, via wiring, to a location where a visible and/or audio alarm would be activated at a console. This console would provide information that would identify the classroom where the panic button was activated, but not who activated it. A more advanced system may incorporate the PA system, which allows the teacher and the administrative personnel to hold a two-way conversation by using the existing room PA speakers and installed internal wiring. The cost of this system for an average school would be approximately $10,000.

There are several weaknesses to a panic-button system. In a classroom situation, it is possible that the panic button would not be readily available in a duress situation. It may be across the room from the teacher's desk or even accidentally blocked by furniture or posters. Also, this configuration lends itself to nuisance alarms triggered by mischievous students. This problem can be offset by hiding the pushbutton or

Exhibit 5.1. This illustration shows a simple duress system for a school's front office. Every public school needs some method of contacting the police quickly and automatically in the event of a true emergency, without having to rely on the public telephone system.

requiring a teacher to enter a PIN on a keypad before use. (The latter is not recommended for schools because of the potential liability of a student attempting, unsuccessfully, to summon help in a threatening situation.) Such a system does not actually identify the person using it, only the owner of the device, but does locate the alarm to a particular classroom or wherever the pushbutton is physically mounted. A panic-button system is cost-effective when installed during the school's initial construction, rather than as a retrofit, and can be a simple and effective system for many types of emergencies.

A second type of system incorporates a pagerlike device that has a panic button built in and is either worn by school personnel or may be installed within a foot switch located under a desk. When the panic button is pushed, a wireless alarm signal is sent to the closest installed wireless sensing unit (a type of repeater) which would then send the signal on to the alarm console. The personnel at the console would receive a coded number and this number would correspond to a teacher. This system does not usually give specific locations other than to the general preprogrammed zone of the repeater. Increasing the number of zones requires more wireless sensing units to be installed, which increases the cost and complexity of the system. A major limiting factor for this system is that the pagerlike device must have a clear line of sight to the nearest sensing unit for an accurate transmission. In other words, walls, glass, roofs, floors, and so forth will degenerate the transmitted signal which decreases the precision of identifying an individual under duress.

This type of system may also incorporate a two-way radio built into the pager that would allow communication between the console operator and person under duress, but this larger pager is more awkward to wear. Also, if a school has an existing PA system, a duress system could utilize the existing PA system wiring to send the signal from the sensing unit to the alarm console. This hybrid system would use both wireless and preexisting wires to reduce the hardware and installation costs. An estimated cost for this type of system would be about $50,000.

A third system, a smarter version of the previous system, can identify, locate, and track the person who activated the duress alarm of his or her pager. Again, school personnel would push the panic button in a duress situation, and this action would send a wireless alarm signal to a more sophisticated wireless sensing unit. The sensing unit would forward the signal to the alarm console. An extensive wireless infrastructure identifies, locates, and tracks the pager device (and hence the person under duress) within school property (exhibits 5.2 and 5.3). The electronics and software of such a system produces a positioning symbol on a console panel or maplike display. (Telephone calls to several vendors during the summer of 1998 revealed that these systems generally cost approximately $100,000 for a 40-acre school area.)

Advanced and promising technologies. The Global Positioning Satellite (GPS) technology that is currently identifying, locating, and tracking everything from military soldiers to car rental vehicles has not been shown to be as successful when used inside buildings or

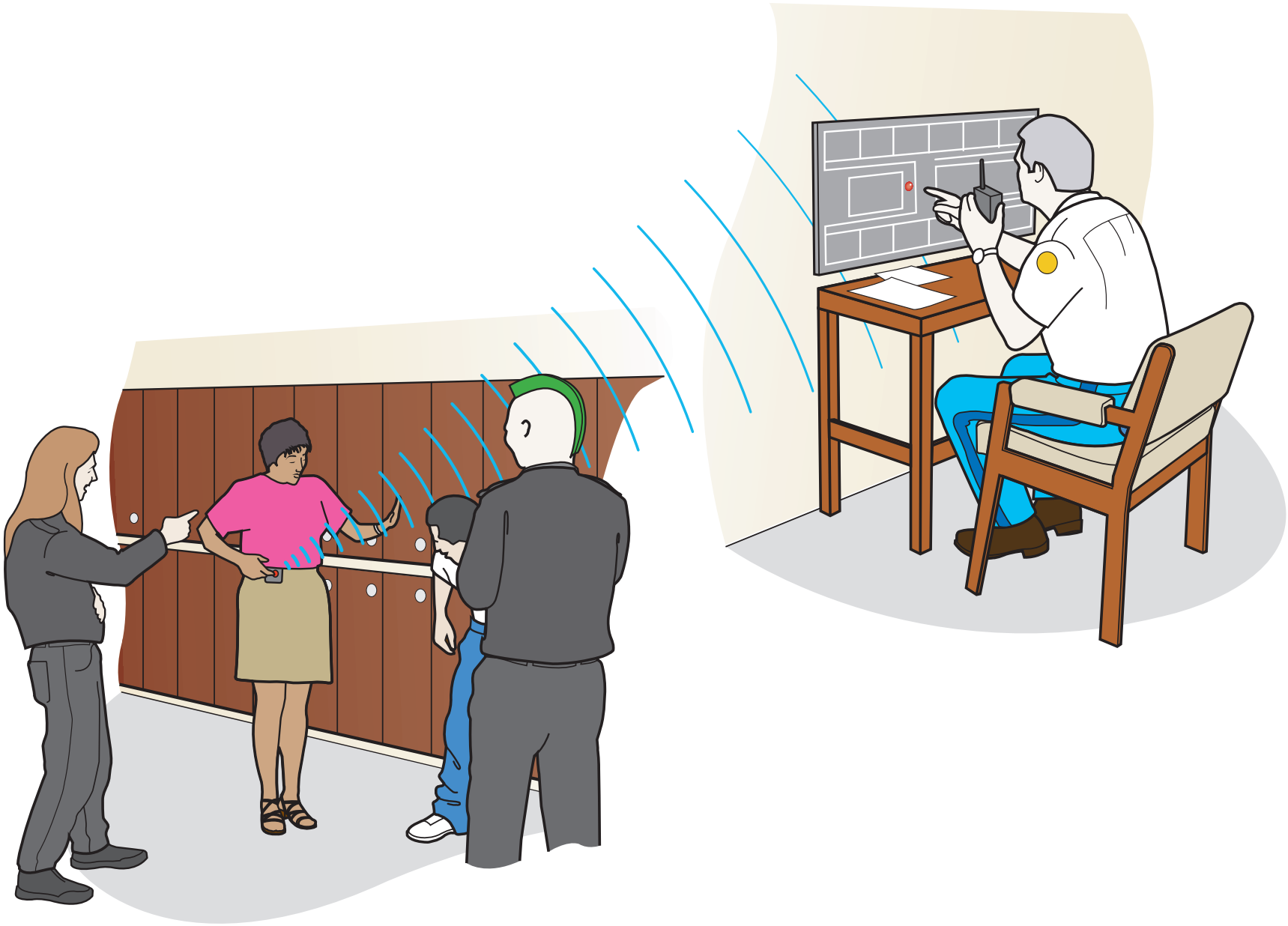


Exhibit 5.2. This illustration depicts the application of a "smarter" duress system that can provide both identification and location information.

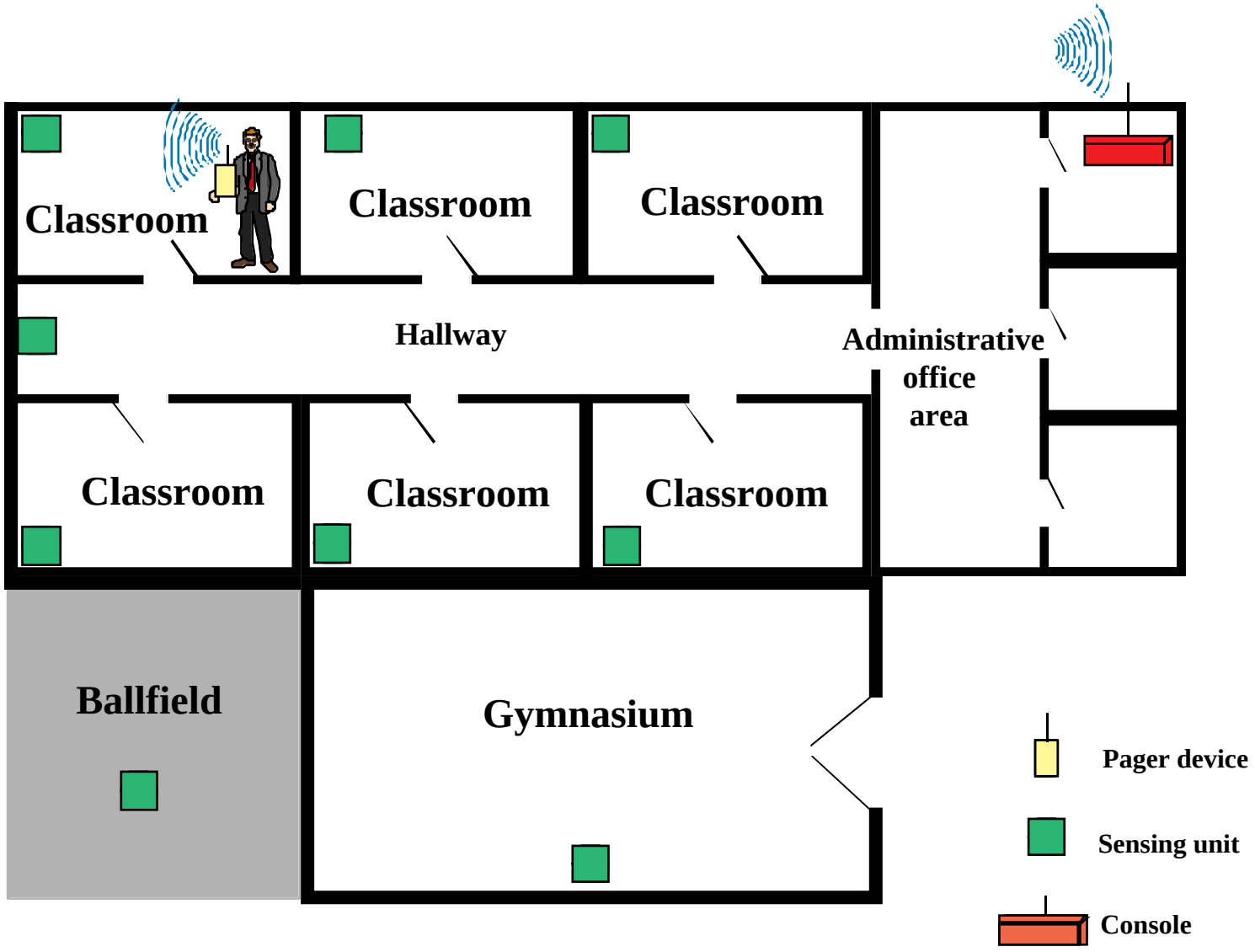


Exhibit 5.3. A sample diagram of the configuration of a duress system.

around large or tall buildings. GPS requires an unobstructed signal from the ground transmitter unit to an Earth-orbiting satellite. Some advanced duress systems use a hybrid design that tracks outside personnel with GPS technology and RF or infrared systems for tracking personnel inside facilities. The cellular phone system infrastructure is improving greatly in capabilities and coverage, which in the future may be a great asset to duress alarm signals. Advances in low earth-orbiting satellite technology that transmits data may also prove to be beneficial in making duress alarm systems more intelligent in the future.

Duress alarm system technologies are improving at a very fast pace but will likely have to come down substantially in cost before they will be affordable to most schools. Before going out on bid for the purchase of such a system, it is recommended that school administrators communicate with current users or request to participate in a demonstration of the proposed system.

Resources: Books, Publications, Web Sites, and Conferences

The list below includes private, professional, and government organizations and publications that are sources of information for school security and safety issues. The list is not exhaustive. It is intended to be representative of the many resources that are now available. Please note that this list includes for-profit organizations as well as not-for-profit entities.

Many public libraries can provide Internet access as a regular patron service if it is not available at your institution.

Education Resources Information Center (ERIC)
2277 Research Blvd., 7A
Rockville, MD 20850
Voice: 301/519–5789
Fax: 301/519–6760
E-mail: acceric@inet.ed.gov
Web site: http://www.aspensys.com/eric

Now under the auspices of the National Library of Education and the Office of Educational Research and Improvement, ERIC produces two monthly indexes, Resources in Education (RIE) and the Current Index to Journals in Education (CIJE). These indexes are available in print, on CD–ROM and via the Internet. The ERIC database, which can be searched via the Internet, now features more than 1 million citations, which include school security, school safety, school violence, legal issues, and the use of technology in these areas.

U.S. Department of Education
600 Independence Ave., S.W.
Washington, DC 20202–0498
Voice: 800/USA–LEARN
Web site: http://www.ed.gov

The Department's Web site contains a wealth of useful information including guides; publications; resource directories; the full text of some Department publications, such as *Early Warning, Timely Response: A Guide to Safe Schools;* and links to other useful sites.

Safe and Drug-Free Schools Program
Office of Elementary and Secondary Education
U.S. Department of Education
600 Independence Ave., N.W.
Washington, DC 20202–6123
Voice: 202/260–3954
Fax: 202/260–7767
Web site: http://www.ed.gov/offices/OESE/SDFS

National Criminal Justice Reference Service (NCJRS)
P.O. Box 6000
Rockville, MD 20849–6000
Voice: 800/851–4320 or 301/519–5500
E-mail: askncjrs@ncjrs.org
Web site: http://www.ncjrs.org

One of the most extensive sources of information on criminal and juvenile justice in the world. NCJRS is a collection of clearinghouses supporting all bureaus of the U.S. Department of Justice Office of Justice Programs, which includes the Office of Juvenile Justice and Delinquency Prevention.

Among the NCJRS services that are available through its Web site are:

Justice Information Center (JIC) with links to resources on many specific topics including juvenile justice and drugs and crime.

NCJRS Abstracts Database, which provides summaries of criminal justice literature—government reports, journal articles, books, and more—and which is searchable free on the Web.

National School Safety Center (NSSC)
4165 Thousand Oaks Blvd., Suite 290
Westlake Village, CA 91362
Voice: 805/373–9977
Fax: 805/373–9277
Web site: http://www.nssc1.org

A nonprofit partnership of the U.S. Department of Justice, the U.S. Department of Education, and Pepperdine University, NSSC was created in 1984 with the charge to promote safe schools—free of crime and violence—and to help ensure quality education for all American children.

NSSC has a number of publications, films/tapes, and posters available for sale. SEE ALSO: Publications.

National Alliance for Safe Schools (NASS)
P.O. Box 1068
College Park, MD 20741
Voice: 301/935–6063
Fax: 301/935–6069
E-mail: nass@erols.com
Web site: http://www.safeschools.org

Founded in 1977 by a group of school security directors to provide technical assistance, training, and research to school districts interested in reducing school-based crime and violence.

NASS products and services include school security assessments; educational programs for troubled youth; training programs for administrators, teachers, and students; various publications; and safe school workshops, which are held at different locations around the country. The NASS Web site includes descriptions of the workshops and a 2–3 month calendar of workshop locations. SEE ALSO: Publications.

National Crime Prevention Council
1700 K St., N.W., Second Floor
Washington, DC 20006–3817
Voice: 202/466–6272
Fax: 202/296–1356
Web site: http://www.ncpc.org or www.weprevent.org

An organization dedicated to helping millions of people across the United States prove that building a sense of community and taking commonsense precautions can cut crime and counter fear.

A major thrust of the Council is “stopping school violence” with many useful suggestions and links included on their Web site.

Keep Schools Safe
Contact: Attorney General of each State
Web site: http://www.keepschoolssafe.org

A joint initiative of the National Association of Attorneys General and the National School Boards Association, which have joined together to address the escalating problem of youth violence.

The Web site was launched to facilitate sharing of ideas and program information by providing up-to-date information on successful programs and ideas.

Center for the Prevention of School Violence
20 Enterprise St., Suite 2
Raleigh, NC 27607–7375
Voice: 800/299–6054 or 919/515–9397
Fax: 919/515–9561
E-mail: Available from Web site
Web site:
http://www2.ncsu.edu/ncsu/cep/PreViolence/CtrPreVio

Established in 1993 at North Carolina State University, the Center serves as a primary point of contact for dealing with the problem of school violence. The Center is currently working on several special projects and is a nationally recognized resource for school resource officer (SRO) programs.

National School Boards Association
1680 Duke St.
Alexandria, VA 22314
Voice: 703/838–6722
Fax: 703/683–7590
E-mail: info@nsba.org
Web site: http://www.nsba.org

A nationwide advocacy outreach organization for public school governance. The Web site provides links to information services of the organization, including its **Council of School Attorneys** and **Keep Schools Safe**, a joint effort with the National Association of Attorneys General.

American Association of School Administrators (AASA)
1801 North Moore St.
Arlington, VA 22209
Voice: 703/528–0700
E-mail: phouston@aasa.org
Web site: http://www.aasa.org

One of elementary and secondary education's longstanding professional organizations. Strives for the development of highly qualified leaders and supporting excellence in educational administration. Initiates and supports laws, policies, research, and practices that will improve education.

National Association of School Resource Officers (NASRO)
P.O. Box 40
Boynton Beach, FL 33425–0040
Voice: 888/316–2776
Web site: http://www.rt66.com/nasro

A nonprofit organization made up of school-based law enforcement officers and school administrators. The association serves as the largest training organization for school-based police and district personnel in the Nation. NASRO sponsors an annual training conference each summer and regional training throughout the year. SEE ALSO: Conferences/meetings.

National Association of School Safety and Law Enforcement Officers
P.O. Box 118
Catlett, VA 20119–0118
Voice: 540/788–4966

An organization of persons engaged in school security and school police operations.

International Association of Campus Law Enforcement Administrators
638 Prospect Ave.
Hartford, CT 06105–4298
Voice: 860/586–7517
E-mail: info@iaclea.org
Web site: http://www.iaclea.org

The membership of this association includes campus law enforcement directors and staff, criminal justice faculty members, municipal chiefs of police, companies offering

campus law enforcement products and services, and colleges and universities throughout the United States, Canada, and the United Kingdom.

Campus Safety Association
1121 Spring Lake Drive
Itasca, IL 60143–3201
Voice: 708/775–2026

Members of this organization are professionals concerned with safety at educational institutions.

American Society for Industrial Security (ASIS)
1625 Prince St.
Alexandria, VA 22314
Voice: 703/522–5800
Fax: 703/243–4954
Web site: http://www.asisonline.org

A primary focus of this organization is to increase the effectiveness and productivity of security professionals by developing educational programs and materials that focus on the fundamentals as well as the latest advancements in security management. ASIS sponsors a variety of educational courses and seminars, an annual national seminar and exhibit, numerous publications, a trade journal, and a security industry buyer's guide.

Educational Institutions is an ASIS standing committee. The ASIS Web site has a great deal of information, including full text of various documents. SEE ALSO: Publications and Conferences/meetings.

International Association of Professional Security Consultants (IAPSC)
1444 I St., Suite 700
Washington, DC 20005–2210
Voice: 202/712–9043
Fax: 202/216–9646
Web site: http://www.iapsc.org

A nonprofit professional association of independent, nonproduct-affiliated, professional security consultants. The IAPSC Web site includes a directory of experts; full text of the current issue of the association newsletter; and information on events and other services. SEE ALSO: Conferences/meetings.

Teacher's Workshop
1250 Overlook Ridge
Bishop,GA 30621
Voice: 800/991–1114
Fax: 706/769–4137
E-mail: rbender@teachersworkshop.com
Web site: http://www.teachersworkshop.com

A source of practical staff development opportunities through teleconferencing, a speaker's bureau, video curricula, or special conference events. The Teacher's Workshop Web site includes information on the various categories of opportunities offered. Each category includes topics on school violence and its prevention. SEE ALSO: Publications.

National School Safety and Security Services (NSSSS)
P.O. Box 110123
Cleveland, OH 44111
Voice: 216/251–3067
E-mail: KENTRUMP@aol.com
Web site: http://www.schoolsecurity.org

An independent, Ohio-based, National consulting firm specializing in training and technical assistance on secondary and elementary (K–12) school security, crisis management, gangs, juvenile crime issues, and crisis preparedness.

NSSSS services include presentations and training; security assessments; expert witness and litigation consultation; and related management consulting. The NSSSS Web site includes information on services, links to other useful sites, and a regularly updated list of publications related to NSSSS service areas. SEE ALSO: Publications.

General Web Sites

NOTE: There are hundreds of Web sites that contain valuable information and resources on the topics of school security, school safety, school violence and prevention, and so forth, and more are added every week. We could not begin to include them all. In addition to the sites included with their organization above, listed below are a few general sites that contain many links to school security information:

National Clearinghouse for Educational Facilities (NCEF)
Web site: http://www.edfacilities.org

With its mission to serve as a resource for the Nation's school personnel and allied professionals who plan, design, construct, and maintain educational facilities, NCEF acquires, manages, and disseminates information relating to educational facilities.

The Clearinghouse is sponsored by the U.S. Department of Education's National Library of Education. Subtopic links at this site include safety and lighting.

Mickey's Place in the Sun—Violence and Violence Prevention
Web site:
http://people.delphi.com/mickjyoung/violence.html

Each of the 14 subtopic links for this Topic include organizations, publications, and other resource links.

BASA–TECH Webliography
Web site:
http://www.nettech.org/basics/projects/weblio.htm

An annotated listing of education-related Web sites.

Security Magazine On The Web
Cahners Publishing Company
Fax: 303/470–4546
Web site: http://www.secmag.com

Security Magazine and its sister publication, *Security Distributing & Marketing (SDM) Magazine*, are available in print form. However, the Web site listed here contains a great deal of useful information on a variety of security topics, including advertised security products; school security solutions; a daily news service made up of a network of global news media and business information by topic (e.g., protecting our children and school (K–12) security), which is updated daily and contains full text articles; a new product database; and a list of experts and columnists.

Conferences/meetings

American Society of Industrial Security (ASIS) Annual Seminar & Exhibits

Includes educational sessions, ASIS security marketplace bookstore, and more than 500 exhibiting companies. Attendance: 15,000 or more security professionals

For information contact:
ASIS
1625 Prince St.
Alexandria, VA 22314–2818
703/519–6200

International Association of Professional Security Consultants (IAPSC) Annual Conference

For information contact:
IASPC
1444 I St., Suite 700
Washington, D.C. 20005–2210
Voice: 202/712–9043
Fax: 202/216–9649

Note: This conference is generally held in April.

National Association of School Resource Officers (NASRO) Annual Conference

Largest gathering of school-based police officers and school security professionals in the United States.

For information contact:
NASRO
P.O. Box 40
Boynton Beach, FL 33425–0040
Voice: 888/316–2776

Note: This conference is generally held in July.

International Security Conference & Exposition (ISC EXPO)

Includes leading-edge seminars and workshops that are organized into core conference tracks that reflect major security topics. More than 400 exhibitors showcase security equipment. The seminars and workshops generally include sessions specific to school security. Information specific to the EXPO program and exhibitors is usually available on the Web site about a month prior to the EXPO date.

For information contact:
ISC EXPO
Customer service
Voice: 800/840–5602

NOTE: Many publications, including those of professional organizations, include a list of upcoming meetings/events as a regular feature. In addition, several Web sites, such as the sites for ERIC, NCJRS, ASIS, SIA, and SDM Magazine, have links to lists of upcoming events.

Publications

Note: Many of the publications included below are available through interlibrary loan at a school or public library.

Books/reports

Blauvelt On Making Your Schools Safe, Peter D. Blauvelt, National Alliance for Safe Schools, 1997.

Campus Public Safety and Security: With Guidance As Well for High Schools and Private Secondary Schools, James W. Wensyel, Charles C. Thomas, Ltd., 1987.

Campus Security and Law Enforcement, John W. Powell, et al., American Society for Industrial Security, second edition, 1994.

Combating Fear and Restoring Safety in Schools, June Arnette and Marjorie C. Walsleben, U.S. Department of Justice, 1998 (NCJ 167888).

Creating Safe and Drug-Free Schools: An Action Guide, U.S. Department of Education and U.S. Department of Justice, 1996 (paper and electronic formats).

Crime in the Schools: Reducing Fear and Disorder with Student Problem Solving, Dennis J. Kenney and T. Steuart Watson, Police Executive Research Forum, 1998.

Crime Prevention Through Environmental Design, Crowe, Butterworth-Heinemann, 1991.

Dealing With Youth Violence: What Schools and Communities Need to Know, Rose Duhan-Sells, editor, National Education Service, 1996.

Early Warning, Timely Response: A Guide to Safe Schools, U.S. Department of Education, 1998 (paper and electronic formats).

Educated Public Relations: School Safety 101, National School Safety Center, 1993.

Effective Strategies for School Security, Peter D. Blauvelt, National Association of Secondary School Principals, 1981.

Gangs in Schools: Breaking Up is Hard to Do, National School Safety Center, 1993.

Legal Issues Surrounding Safe Schools, Reed B. Day, National Organization on Legal Problems of Education, 1994.

Maximum Security: The Culture of Violence in Inner-City Schools, John Devine, 1996.

Practical School Security: Basic Guidelines for Safe and Secure Schools, Kenneth Trump, Corwin Press, 1998 (hardcover and paperback).

Safe Schools: A Handbook for Violence Prevention, R.D. Stephens, National Educational Service, 1995.

Safe Schools: A Security and Loss Prevention Plan, James Barry Hylton, Butterworth-Heinemann, 1996.

Safe Schools, Safe Students: A Guide to Violence Prevention, Drug Strategies, Inc., 1998.

Safety and Security Administration in School Facilities: Forms, Checklists & Guidelines, Sara N. DiLima, editor, Aspen Publishers, Inc., 1996.

School Discipline Notebook, National School Safety Center, 1992.

School Safety Check Book, National School Safety Center, 1990.

School Safety Workbook, National School Safety Center, 1996.

School Violence Intervention: A Practical Handbook, J.C. Conoley and A. P. Goldstein, editors, Guilford Publications, Inc., 1997.

Schools, Violence and Society, A.M. Hoffman, editor, the Greenwood Publishing Group, 1996.

Student Searches and the Law, National School Safety Center, 1996.

Techniques for Managing a Safe School, Beverley H. Johns and John P. Keenan, Love Publishing Co., 1997.

Teens, Crime, and the Community: Education and Action for Safe Schools and Communities, Judy Zimmer, et al., West Educational Publishing, third edition, 1998.

Toward Better and Safer Schools, A.G. Cuervo, et al., National School Boards Association, 1985.

Violence Prevention and Reduction in Schools, William Bender (et al), editor, PRO ED, Inc., Spring 1999.

Journals/newsletters

The American School Board Journal, monthly, National School Boards Association, 1680 Duke St., Alexandria, VA 22314, 703/838–6722, info@nsba.org, www.nsba.org.

Campus Security Report, monthly, Rusting Publications, 402 Main St., P.O. Box 190, Port Washington, NY 11050, 516/883–1440.

Inside School Safety, monthly, Aspen Publishers, Inc., 7201 McKinney Circle, Frederick, MD, 800/638–8437, www.aspenpublishers.com.

International Association of Campus Law Enforcement Administrators (IACLEA)—Campus Law Enforcement Journal, 638 Prospect Avenue, Hartford, CT 06105, 860/586–7517.

School Safety, three times/year, National School Safety Center, 4165 Thousand Oaks Blvd., Suite 290, Westlake Village, CA 91362, 805/373–9977, www.nssc1.org.

School Security Report, monthly, Rusting Publications, 402 Main Street, P.O. Box 190, Port Washington, NY 11050, 516/883-1440.

Security Distributing & Marketing (SDM) Magazine, monthly, Cahners Publishing Company, 1350 E. Touhy Ave., Des Plaines, IL 60018–3358 (Frequently includes articles on school security).

Security Magazine, monthly, Cahners Publishing Company, 1350 E. Touhy Ave., Des Plaines, IL 60018–3358, www.secmag.com (Frequently includes articles on school security).

Security Management, monthly, American Society for Industrial Security, 1625 Prince St., Alexandria, VA 22314, 703/522–5800, www.asisonline.org.

Security News, monthly, Terra Publishing, Inc., 4250 North State St., Salamanca, NY 14779–9700, 716/945–5091 (Frequently includes articles on school security).

Security Technology & Design, quarterly, Locksmith Publishing Corp., 850 Busse Highway, Park Ridge, IL 60068, 708/692–5940, www.simon-net.com/asp/library.asp?Provider ID=23 (Frequently includes articles on school security).

Updating School Board Policies, National School Boards Association, 1680 Duke St., Alexandria, VA 22314, 703/838–6722, info@nsba.org, www.nsba.org. (Frequently includes articles on school security).

Directories

Thomas Register of American Manufacturers, A directory of 150,000 U.S. and Canadian manufacturers and their products available in paper and/or CD format at many large public libraries and available free on the Internet. The directory is searchable on the Internet by company name, product name, or brand name. An easy, free registration is required before searching.

American Society for Industrial Security (ASIS) Security Industry Buyer's Guide, An annual directory that is available with a subscription to *Security Management*. It is searchable by type of equipment.

National Security Institute Product & Services Directory, An online directory searchable by company type and/or product and services. Listings in the directory are available free of charge to appropriate vendors.

Security Industry Association (SIA) Membership Directory, Directory of manufacturers, distributors, and service companies in the electronic security industry. Available for a fee to nonmembers.

Security Industry Association (SIA) Directory of Specialists, Directory of security professionals that is indexed by specialty area and geographic region. Available for a fee to nonmembers.

About the National Institute of Justice

The National Institute of Justice (NIJ), a component of the Office of Justice Programs, is the research agency of the U.S. Department of Justice. Created by the Omnibus Crime Control and Safe Streets Act of 1968, as amended, NIJ is authorized to support research, evaluation, and demonstration programs, development of technology, and both national and international information dissemination. Specific mandates of the Act direct NIJ to:

- Sponsor special projects, and research and development programs, that will improve and strengthen the criminal justice system and reduce or prevent crime.
- Conduct national demonstration projects that employ innovative or promising approaches for improving criminal justice.
- Develop new technologies to fight crime and improve criminal justice.
- Evaluate the effectiveness of criminal justice programs and identify programs that promise to be successful if continued or repeated.
- Recommend actions that can be taken by Federal, State, and local governments as well as by private organizations to improve criminal justice.
- Carry out research on criminal behavior.
- Develop new methods of crime prevention and reduction of crime and delinquency.

In recent years, NIJ has greatly expanded its initiatives, the result of the Violent Crime Control and Law Enforcement Act of 1994 (the Crime Act), partnerships with other Federal agencies and private foundations, advances in technology, and a new international focus. Some examples of these new initiatives:

- New research and evaluation are exploring key issues in community policing, violence against women, sentencing reforms, and specialized courts such as drug courts.
- Dual-use technologies are being developed to support national defense and local law enforcement needs.
- The causes, treatment, and prevention of violence against women and violence within the family are being investigated in cooperation with several agencies of the U.S. Department of Health and Human Services.
- NIJ's links with the international community are being strengthened through membership in the United Nations network of criminological institutes; participation in developing the U.N. Criminal Justice Information Network; initiation of UNOJUST (U.N. Online Justice Clearinghouse), which electronically links the institutes to the U.N. network; and establishment of an NIJ International Center.
- The NIJ-administered criminal justice information clearinghouse, the world's largest, has improved its online capability.
- The Institute's Drug Use Forecasting (DUF) program has been expanded and enhanced. Renamed ADAM (Arrestee Drug Abuse Monitoring), the program will increase the number of drug-testing sites, and its role as a "platform" for studying drug-related crime will grow.
- NIJ's new Crime Mapping Research Center will provide training in computer mapping technology, collect and archive geocoded crime data, and develop analytic software.
- The Institute's program of intramural research has been expanded and enhanced.

The Institute Director, who is appointed by the President and confirmed by the Senate, establishes the Institute's objectives, guided by the priorities of the Office of Justice Programs, the Department of Justice, and the needs of the criminal justice field. The Institute actively solicits the views of criminal justice professionals and researchers in the continuing search for answers that inform public policymaking in crime and justice.