

Course Instructions

NOTE: The following pages contain a preview of the final exam. This final exam is identical to the final exam that you will take online after you purchase the course.

After you purchase the course online, you will be taken to a receipt page online which will have the following link: [Click Here to Take Online Exam](#). You will then click on this link to take the final exam.

3 Easy Steps to Complete the Course:

- 1.) Read the Course PDF Below.**
- 2.) Purchase the Course Online & Take the Final Exam – see note above**
- 3.) Print Out Your Certificate**

Design of Schools in Case of Terrorist Attacks and School Shootings - Final Exam

- 1. With regards to 1.2 Risk Assessment, IRVS is:**
 - a. an older school security system
 - b. too costly for most school districts
 - c. the latest risk assessment methodology
 - d. being replaced by newer technology

- 2. IRVS is a quick assessment tool for obtaining a preliminary risk assessment rating.**
 - a. True
 - b. False

- 3. A Threat Rating of 7 (Table 1-3) is considered:**
 - a. medium high
 - b. very low
 - c. high
 - d. very high

- 4. Considering Vulnerability Assessment (1.2.2.3), three main aspects of a school's vulnerability must be taken into account:**
 - a. Structural, Infrastructure, Financial
 - b. Structural, Nonstructural, Organizational
 - c. Site, Entrance, Circulation
 - d. none of the above

- 5. Organizational Vulnerabilities include characteristics of school spatial organization as well as operational and procedural routines that may be exploited by the attackers.**
 - a. True
 - b. False

- 6. DHS has designated the _____ as the lead agency for school-related security:**
 - a. National Security Agency
 - b. Federal Bureau of Investigation
 - c. Government Investigations Office
 - d. U.S. Department of Education

7. As a result of the massive expansion of the suburbs of large cities following World War II (from 2.2.1), and the continued existence of small towns, most U.S. schools are located:

- a. in urban areas.
- b. in impoverished neighborhoods
- c. near former industrial areas
- d. on suburban/rural sites

8. With regards to Topography, schools in high-risk zones may require additional protection immediately adjacent to the structure in the form of a clear zone, free of all topographic obstructions or even landscaping that might provide hiding places.

- a. True
- b. False

9. Considering Layers of Defense (2.3.3), this document emphasizes _____ main layers:

- a. two
- b. three
- c. seven
- d. four

10. A *Perimeter Security* system consists of two main elements.

- a. True
- b. False



Buildings and Infrastructure Protection Series

Primer

to Design Safe School Projects
in Case of Terrorist Attacks and School Shootings

FEMA-428/BIPS-07/January 2012

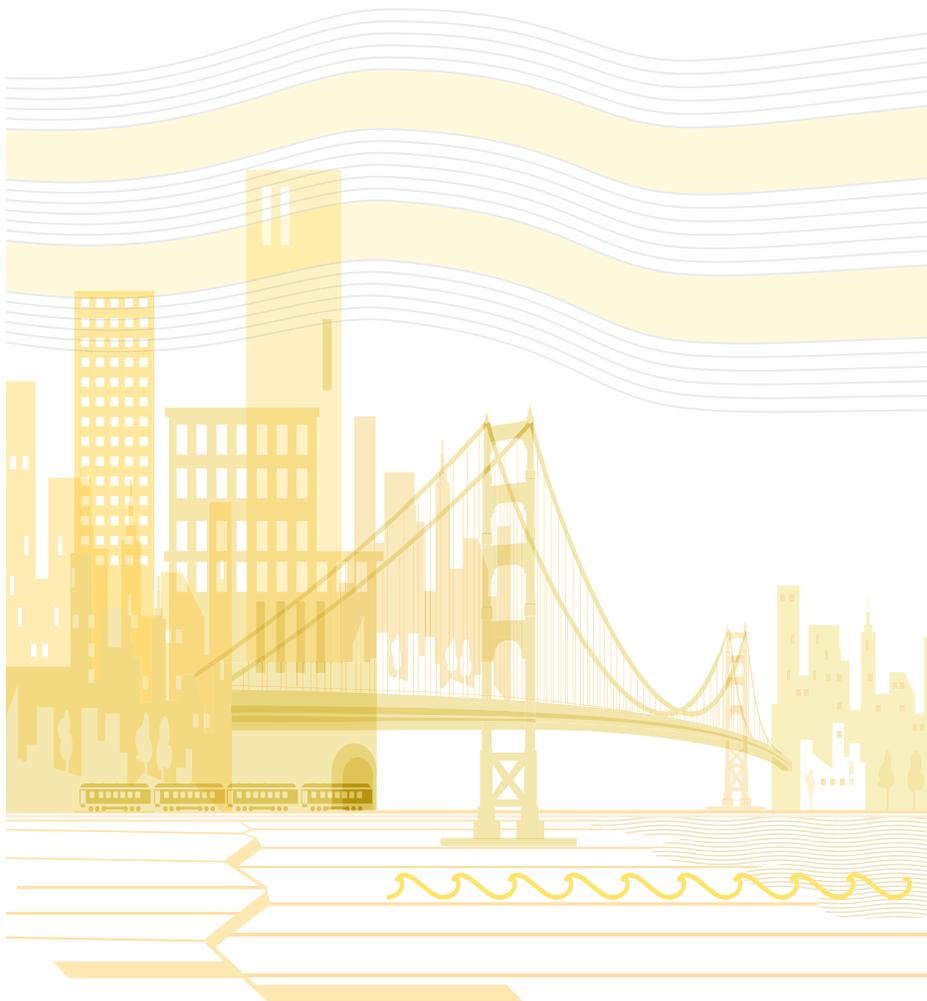
Edition 2



**Homeland
Security**

Science and Technology

Risks for Schools



In this chapter:

This chapter discusses the key aspects of security risk management with an emphasis on risk assessments. It introduces two methodologies developed by U.S. Department of Homeland Security (DHS) Science and Technology (S&T) Directorate that can be used for the assessment of school risks, but focuses primarily on the method based on FEMA 452, *Risk Assessment: A How-To Guide to Mitigate Potential Terrorists Attacks* (2005). Given the specific nature of educational facilities, this primer includes a customized checklist for schools.

Although school building designs have evolved dramatically over the years, schools continue to be open and accessible places that offer opportunities for study, work, and play. Unfortunately, the openness and inviting environment of schools create opportunities for intruders with malicious intent. Violent attacks on students and teachers in the Nation's schools are extremely rare events, but their effects frequently, and understandably, have far-reaching consequences. Most parents' anxieties are not assuaged by statistics showing low probabilities of serious incidents. Consequently, security at schools has become a subject of widespread public concern. Introducing security requirements as

part of school design requires a comprehensive approach to balance many different objectives, such as reducing risks, maintaining open access for students and staff, facilitating proper building function, conforming to aesthetic principles, hardening of physical structures beyond the required buildings codes and standards, and maximizing the use of nonstructural systems.

This chapter discusses the key aspects of security risk management with an emphasis on risk assessments. It introduces two methodologies developed by U.S. Department of Homeland

Security (DHS) Science and Technology (S&T) Directorate that can be used for the assessment of school risks, but focuses primarily on the method based on FEMA 452, *Risk Assessment: A How-To Guide to Mitigate Potential Terrorists Attacks* (2005). Given the specific nature of educational facilities, this primer includes a customized checklist for schools.

1.1 Risk Management

The management of risk of extreme events that may affect a school, such as terrorist attacks and technological or other manmade disasters, is a process that includes activities to both identify the risks and respond to them. In addition to the process of risk assessment described below, risk management comprises mitigation, preparedness, and response. Rather than focusing on individual aspects of a particular threat or hazard, risk management employs a comprehensive approach to managing intentionally or accidentally caused extreme events, with the intention of reducing risks by addressing all the factors that contribute to that risk.

Although comprehensive risk management guidance is beyond the purview of this primer, understanding the role and significance of each of its components is important. The decisions that affect the security of



The management of risk of extreme events that may affect a school, such as terrorist attacks and technological or other manmade disasters, is a process that includes activities to both identify the risks and respond to them.

schools are made at various levels of government and school administration and are based on a variety of criteria. The last portion of this chapter addresses some of the questions and dilemmas that decisionmakers face.

1.2 Risk Assessment

This section presents methodologies for school administrators, planners, architects, engineers, and other building science professionals to identify and quantify the security risks to which a school may be exposed. The ultimate objective of the risk assessment process is to find the most effective mitigation measures to achieve a desired level of protection against terrorist and other kinds of attacks. These methodologies will help both school administrators and designers to define and evaluate threats, consequences, and vulnerabilities for the purpose of integrating the security risks into an effective design strategy. Understanding the risks will help school administrators prioritize their mitigation activities and allocate their resources accordingly, and will help architects, engineers, and security experts identify the most cost-beneficial protective measures to reduce the risk for a school's unique security needs. The methodologies described in this chapter can be used during the design process for new and existing school buildings that are undergoing renovation.

The first part of this section describes the latest risk assessment methodology, called Integrated Rapid Visual Screening (IRVS), devised by the S&T Directorate. The remaining parts of this section describe the risk assessment methodology described in FEMA 452.

1.2.1 Integrated Rapid Visual Screening

The S&T Directorate has developed an IRVS procedure for assessing risks to all types of buildings from natural and manmade hazards with the potential to cause catastrophic losses. The procedure is an enhanced version of the screening process described in FEMA 455, *Handbook for Rapid Visual Screening of Buildings to Evaluate Terrorism Risk* (2009), and includes improvements to the methodology, updates to the catalog of building characteristics, and updates to the forms to incorporate natural hazards, building types, and critical functions. IRVS has become a very popular tool, mainly because of its simplicity and accuracy, for conducting pre-assessments of schools' susceptibility to threats and hazards.



The ultimate objective of the risk assessment process is to find the most effective mitigation measures to achieve a desired level of protection against terrorist and other kinds of attacks.



The IRVS procedure was developed to assess risks to all types of buildings from natural and manmade hazards with the potential to cause catastrophic losses.



IRVS is a quick assessment tool for obtaining a preliminary risk assessment rating.

IRVS is a quick assessment tool for obtaining a preliminary risk assessment rating. The natural and manmade hazards considered in the tool include: internal and external explosive attacks; ballistic attacks; external chemical, biological, and radiological (CBR) releases; earthquakes; high winds; floods; landslides; and fires. Risk is

determined by evaluating key building characteristics to identify threats, consequences, and vulnerabilities. Experts can use the information from the visual inspection to support higher level assessments and analysis of mitigation options.

The latest improvements to the IRVS database software have made the IRVS methodology completely digital (Figure 1-1). The software facilitates data collection and functions as a data management tool. Assessors can use the software on a PC tablet or laptop to collect, store, and report screening data systematically. The software can be used during all phases (pre-field, field, and post-field) of the IRVS procedure. For more information on IRVS, please visit the S&T Directorate's Web site for Building and Infrastructure Protection Tools: <http://www.dhs.gov/files/programs/scitech-bips-tools.shtm#4>.

Figure 1-1: IRVS database

The screenshot displays the 'iRVS Site Record' software interface. The top section contains various input fields for facility information, including Facility Name (pre-filled with 'Building ABC'), Facility ID#, Org. Name, Address1, Address2, City, St, Zip, Sector, Facility Importance, Site Type (pre-filled with 'Building'), and Subsector. A 'Default Facility Image' dropdown is set to 'No Image Available'. Below these fields is a section for 'Assessment(s)' with a 'Coordinates' tab. A table with the following columns is visible: 'Assessment Number', 'Assessment Date *', 'Assessment Comments / Notes', 'Assessment Folder Name', and 'Enter By'. The table contains one row with the value '01' in the 'Assessment Number' column. At the bottom of the interface, there are two buttons: 'Create additional (blank) assessment record for this site' and 'Create a duplicate of Screening [01] including scoring'. A status bar at the very bottom shows 'Record: 1 of 1', 'No Filter', and a 'Search' field. A legend indicates that fields with an asterisk are required.

The IRVS tool is the first and only software to quantify a building's overall risk score in terms of a 1) resilience score and 2) a multi-hazard risk score based on a few hours of guided screening guided using the IRVS tool. Scoring for risk and resilience is based on a methodology that uses built-in weights and predefined algorithms for final scoring.

Resilience Score: Resilience is computed using three basic components—robustness, resourcefulness, and recovery (the 3 R’s)—based on downtime and operational capacity (Figure 1-2). Analysis of continuity of operations and operational resilience are key to determining the resilience of the building.

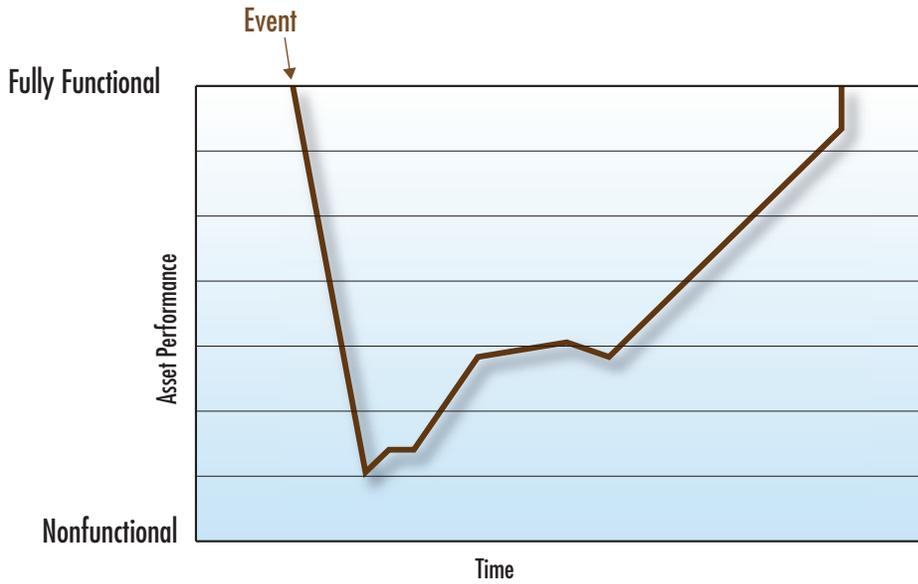


Figure 1-2:
Example of resilience

Multi-Hazard Risk Score: IRVS methodology determines the level of risk to a building from both natural and manmade hazards. A list of these hazards is provided in Table 1-1.

Table 1-1: IRVS Threat Types and Scenarios

Threat Type	Threat Scenario
Internal Attack	Explosive Attack
	CBR Release
	Intrusion
External Explosive Attack	External Zone I Explosive Attack
	External Zone II Explosive Attack
	External Zone III Explosive Attack
External CBR Release	External Zone I CBR Release
	External Zone II CBR Release
	External Zone III CBR Release
Earthquake	Ground Shaking
	Ground Failure
Flooding	Stillwater
	Velocity Surge

Threat Type	Threat Scenario
Wind	Hurricane (Wind and Water)
	Tornado
	Other High Wind
Landslide	Rainfall
Fire	Resulting from Earthquake
	Resulting from Blast
	Arson or Incidental

Note: Zone I is within 100 feet of the building; Zone II is from 100 to 300 feet of the building; and Zone III is from 300 to 1000 feet of the building.

One or two screeners can conduct and complete a screening in 1 to 5 hours. The IRVS operates on Microsoft (MS) Access 2007 with support from MS Excel 2007 and MS Word 2007, as well as PDF files. The software tool facilitates data collection and data management functions. Screeners use the software tool on a PC tablet or laptop to collect, store, and report screening data. The software tool can be used during all phases of the IRVS procedure (pre-field, field, and post-field). Data collected

during the screening are transferred to a database and stored as individual records, which are used to compute the risk score.



One or two screeners can conduct and complete a screening in 1 to 5 hours.

The digital catalog guides the user through each of the screening questions.

The digital catalog guides the user through each of the screening questions in the assessment with background information to assist with answering the question. Screeners will need to become familiar with the catalog to maintain accuracy and consistency from one assessment to another. The

reliability and quality of the screening depends on the amount of time devoted and the quality of information collection. The reliability and quality can be increased if screeners verify structural, mechanical, and security features, perform interior inspections, conduct interviews with security and other key personnel, and review drawings and security operation manuals.



The final product provides a color-coded legend, and a number of scores (risk, resiliency, threat, vulnerability, consequence, etc.).

The final product provides a color-coded legend, and a number of scores (risk, resiliency, threat, vulnerability, consequence, etc.) in whole numbers. The tool also allows the assessor to duplicate the assessment and add additional countermeasures to demonstrate to tenants what effect a countermeasure will have on an overall score.

FEMA 455 describes a rapid visual screening procedure, effectively a “Pre-Tier 1” assessment. The assessment is designed to be conducted by one or two screeners and, depending on the level of effort and access to building information, can be completed in as little as a few hours or as much as 2 days. The S&T Directorate has expanded FEMA 455 to include natural hazards with the development of IRVS.

FEMA 452 outlines methods for identifying the critical assets and functions within buildings, determining the threats to those assets, and assessing the vulnerabilities associated with those threats. Tier 1 is a “70 percent” assessment, while Tier 2 represents a “90 percent” assessment solution.

IRVS facilitates the comparison of the national building inventory independent of the region, multihazard exposure, and type of building. These results can be used to prioritize buildings for further assessment or mitigation, allowing for an efficient allocation of resources. IRVS is also intended to be used to identify the level of risk and resilience for a facility, as the basis for prioritization for further risk management activities and to support higher level assessments and mitigation options by experts.

1.2.2 Risk Assessment Based on FEMA 452

The main goal of the FEMA 452 approach is to help identify most cost-beneficial (in terms of effectiveness) protective measures for a school building’s unique safety and security needs. Figure 1-3 depicts the risk assessment process model from which FEMA 452 methodology and its components originated. Section 1.2.2.1 describes how to identify and define the main threats and hazards to which a school may be exposed. Section 1.2.2.2 discusses the potential magnitude of losses of assets, such as people, buildings, equipment, and functions, recognizing that students, faculty, and staff will always be a school’s most vital asset requiring protection. Section 1.2.2.3 discusses how to perform a vulnerability assessment to identify weaknesses that might exacerbate losses and could be exploited by a terrorist or attacker. The final step in the process is risk analysis, discussed in Section 1.2.2.4, which combines the results of the threat, consequences, and vulnerability assessments to determine the degree of the school’s risk exposure.

Risk assessment of a school is best performed by security professionals who are experts in risk management, building design, blast effects, and CBR incidents, as well as the latest law enforcement and antiterrorism security measures. If hiring professionals is not feasible, members of the design community and/or school administrators can perform an assessment using the methodology presented in this primer. A key tool in the assessment process, the School Vulnerability Assessment Checklist, is provided in Appendix F.

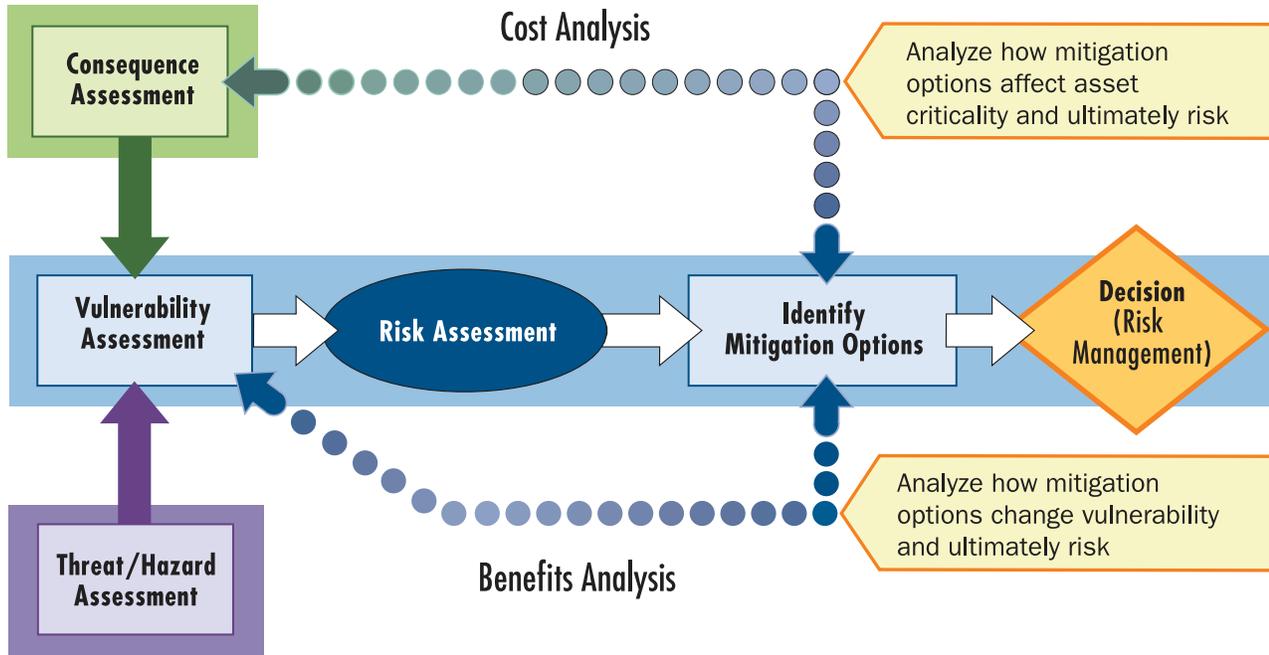


Figure 1-3: Risk assessment process model

1.2.2.1 Threat Assessment

The threat originates from people or organizations that have both the intent and capability to do harm. They may seek publicity for their cause or political gain through their actions to injure or kill people, or to destroy or damage facilities, property, equipment, or resources. For purposes of risk assessment and mitigation of risk, knowing how a school might be attacked is more important than by whom or why. When a risk assessment is conducted for a particular school, defining threats in terms of the types of attacks that may be expected is more useful than attempting to identify the attackers or the reasons why they would want to attack a particular school. Consequently, the methodology for threat analysis and risk assessment proposed in this primer focuses on threats defined as attack types regardless of their origin or cause.

In addition to intentional attack types of threats, this primer also considers various types of hazards. Hazards are defined in several contexts: natural, manmade, or technological. Natural hazard typically refers to a source of harm or difficulty created by a meteorological, environmental, or geological phenomenon or combination of phenomena, such as earthquakes, flooding, fires, lightning, and winds that can affect a school. Manmade hazards, or technological hazards, and terrorism are distinguished from natural hazards in that they originate from human activity. Technological hazards are generally assumed to be accidental and their

consequences unintended, while the willful harmful human activities are described as “threats.” For the sake of simplicity, this primer will use the term “threat” for intentional acts and “hazard” when referring to natural hazards and technological accidents respectively.



Risk assessment starts with the identification and definition of threats and tactics that may be employed in an attack.

FEMA 452 methodology is devoted to the compilation and analysis of available information concerning threats and technological hazards. Risk assessment starts with the identification and definition of threats and tactics that may be employed in an attack. Schools are typically site-constrained, have well defined traffic control and entry points, and operate on standard schedules. Designers and school administrators need to evaluate attack objectives, threat event profiles, and the potential effects of the attack on the school and its occupants. Table 1-2 provides a broad spectrum of manmade threats/hazards to consider and can be used as a tool in the threat assessment process. An extensive list of potential chemical and biological agents that can be used in terrorist attacks is provided in Appendix C. Explosive blast effects are discussed in Chapter 4.

Table 1-2: Event Profiles for Terrorism and Technological Hazards

Threat/Hazard	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Improvised Explosive Device (Bomb) <ul style="list-style-type: none"> • Stationary Vehicle • Moving Vehicle • Mail • Supply • Thrown • Placed • Suicide Bomber 	Detonation of explosive device on or near target; via person, vehicle, or projectile.	Instantaneous; additional secondary devices may be used, lengthening the duration of the threat/hazard until the attack site is determined to be clear.	Extent of damage is determined by type and quantity of explosive. Effects generally static other than cascading consequences, incremental structural failure, etc.	Blast energy at a given stand-off is inversely proportional to the cube of the distance from the device; thus, each additional increment of stand-off provides progressively more protection. Exacerbating conditions include ease of access to target; lack of barriers/shielding; poor construction; and ease of concealment of device.
Armed Attack <ul style="list-style-type: none"> • Ballistics (small arms) • Stand-off Weapons (rocket propelled grenades, mortars) 	Tactical assault or sniper attacks from a remote location.	Generally minutes to days.	Varies, based upon the perpetrator’s intent and capabilities.	Inadequate security can allow easy access to target, easy concealment of weapons, and undetected initiation of an attack.

Threat/Hazard	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Chemical Agent <ul style="list-style-type: none"> • Blister • Blood • Choking/ Lung/ Pulmonary • Incapacitating • Nerve • Riot Control/ Tear Gas • Vomiting 	Liquid/aerosol contaminants can be dispersed using sprayers or other aerosol generators; liquids vaporizing from puddles/containers; or munitions.	Chemical agents may pose viable threats for hours to weeks, depending on the agent and the conditions in which it exists.	Contamination can be carried out of the initial target area by persons, vehicles, water, and wind. Chemicals may be corrosive or otherwise damaging over time if not remediated.	Air temperature can affect evaporation of aerosols. Ground temperature affects evaporation in pools of liquids. Humidity can enlarge aerosol particles, reducing the inhalation hazard. Precipitation can dilute and disperse agents, but can spread contamination. Wind can disperse vapors, but also cause target area to be dynamic. The micro-meteorological effects of buildings and terrain can alter travel and duration of agents. Shielding in the form of sheltering in place may protect people and property from harmful effects for a limited time.
Biological Agent <ul style="list-style-type: none"> • Anthrax • Botulism • Brucellosis • Plague • Smallpox • Tularemia • Viral Hemorrhagic Fevers • Toxins (Botulinum, Ricin, Staphylococcal Enterotoxin B, T-2 Mycotoxins) 	Liquid or solid contaminants can be dispersed using sprayers/aerosol generators or by point or line sources such as munitions, covert deposits, and moving sprayers. May be directed at food or water supplies.	Biological agents may pose viable threats for hours to years, depending on the agent and the conditions in which it exists.	Depending on the agent used and the effectiveness with which it is deployed, contamination can be spread via wind and water. Infection can be spread via human or animal vectors.	Altitude of release above ground can affect dispersion; sunlight is destructive to many bacteria and viruses; light to moderate winds will disperse agents, but higher winds can break up aerosol clouds; and the micro-meteorological effects of buildings and terrain can influence aerosolization and travel of agents.
Radiological Agent <ul style="list-style-type: none"> • Alpha • Beta • Gamma 	Radioactive contaminants can be dispersed using sprayers/aerosol generators, or by point or line sources such as munitions, covert deposits, and moving sprayers.	Contaminants may remain hazardous for seconds to years, depending on material used.	Initial effects will be localized to site of attack; depending on meteorological conditions, subsequent behavior of radioactive contaminants may be dynamic.	Duration of exposure, distance from source of radiation, and the amount of shielding between source and target determine exposure to radiation.
Cyber Attacks	Electronic attack using one computer system against another.	Minutes to days.	Generally no direct effects on built environment.	Inadequate security can facilitate access to critical computer systems, allowing them to be used to conduct attacks.

Threat/Hazard	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
High-Altitude Electromagnetic Pulse (HEMP)	An electromagnetic energy field produced in the atmosphere by the power and radiation of a nuclear explosion. It can overload computer circuitry with effects similar to, but causing damage much more swiftly than a lightning strike.	It can be induced hundreds to a few thousand kilometers from the detonation.	Affects electronic systems. There is no effect on people. It diminishes with distance, and electronic equipment that is turned off is less likely to be damaged.	To produce maximum effect, a nuclear device must explode very high in the atmosphere. Electronic equipment may be hardened by surrounding it with protective metallic shielding that routes damaging electromagnetic fields away from highly sensitive electrical components.
High Power Microwave (HPM) Electromagnetic Pulse	It is a non-nuclear radio frequency energy field. Radio frequency weapons can be hidden in an attaché case, suitcase, van, or aircraft. Energy can be focused using an antenna, or emitter, to produce effects similar to HEMP, but only within a very limited range.	An HPM weapon has a shorter possible range than HEMP, but it can induce currents large enough to melt circuitry, or it can cause equipment to fail minutes, days, or even weeks later. HPM weapons are smaller-scale, are delivered at a closer range to the intended target, and can sometimes be emitted for a longer duration.	Vulnerable systems include electronic ignition systems, radars, communications, data processing, navigation, electronic triggers of explosive devices. HPM capabilities can cause a painful burning sensation or other injury to a person directly in the path of the focused power beam, or can be fatal if a person is too close to the microwave emitter.	Very damaging to electronics within a small geographic area. A shockwave could disrupt many computers within a 1-mile range. Radio frequency weapons have ranges from tens of meters to tens of kilometers. Unlike HEMP, however, HPM radiation is composed of shorter wave forms at higher-frequencies, which make it highly effective against electronic equipment and more difficult to harden against.

Note: Cyber attack focuses on denial of service, worms, and viruses designed to attack or destroy critical infrastructure related systems such as energy management, supervisory control and data acquisition systems, security, control valves, and voice over internet protocol telephones, which are critical systems that support multiple functions and are becoming increasingly connected to the internet.

Identification and Quantification of Threats

A threat is any indication, circumstance, or event with the potential to inflict harm and cause losses. A complete description of the threats to which a school may be exposed requires consideration of every mode of attack separately. In practice, focusing on a limited number of representative attack types that are most common, such as active shooter types of attack, attacks with explosive devices, or CBR types of attack, may suffice. The likelihood that any particular threat will be used against the school must be assessed based on the best information available.



A threat is any indication, circumstance, or event with the potential to inflict harm and cause losses.

Unlike historical and quantitative data available on natural hazards, data for manmade hazards may be scarce and are often largely subjective. This is especially true for threats, which are by their very nature volatile and unpredictable. In

most cases in the past, schools were attacked by people closely associated with that facility, such as students or school employees. However, the possibility that schools may be used as proxy targets by attackers that are not in any way related to that school should not be disregarded. The shocking nature of attacks on school children reverberates through a society and may be a sufficient incentive for unscrupulous attackers to try to inflict as much harm as possible.

Once the potential threats/hazards have been identified and defined, the ways these threats/hazards may be realized must be identified and analyzed. Understanding the nature of the threat is not enough—how will that threat be deployed is equally, if not more, important. Most planned attacks usually include advance surveillance, forced entry, in secrecy or by an open attack, or remote activation of a variety of weapons. The attack weapons can include incendiary devices, small arms (rifles and handguns), standoff military-style weapons (rocket-propelled grenades or mortars), explosives, and CBR devices, individually or combined with explosives to aid in dispersion.

Threat Rating

Once a list of potential threats or attack scenarios is compiled, the likelihood that these attacks may take place at that particular location should be considered. In case of threats, the likelihood of occurrence is not easily defined and involves many uncertainties that affect risk assessment decisions. The source of these uncertainties is our imperfect knowledge of the potential attacker's existence, capability, history, intention, or targeting. Often, information is sketchy and analysts must rely on the subjective

judgment of experts to help estimate the likelihood of a particular type of attack. School authorities do not have the capability to conduct their own terrorist threat analysis, and should use the recommendations of experts and their own judgment to estimate the probabilities and assign ratings to various attack types or attack scenarios.

Table 1-3 provides a scale to help with this determination. The scale is a combination of a 7-level nominal scale and a 10-point numerical scale (10 being the greatest threat). The key elements of the scale are the likelihood/credibility of a threat, potential weapons to be used during a terrorist attack, and information available to decisionmakers. Given the extreme volatility of these threat characteristics, and the difficulties in managing them, this primer focuses on the other components of risk, in particular the vulnerabilities of school facilities.

Table 1-3: Threat Rating Scale

THREAT RATING		
Very High	10	Known aggressors or hazards highly capable of causing loss of, or damage to, the school exist. One or more vulnerabilities are present. The aggressors are known or highly suspected of having the intent to exploit the school's assets and are known or highly suspected of performing surveillance on a facility.
High	8–9	Known aggressors or hazards capable of causing loss of, or damage to, the school exist. One or more vulnerabilities are present and the aggressors are known or reasonably suspected of having the intent to exploit the school's assets.
Medium High	7	Known aggressors or hazards capable of causing loss of, or damage to, the school exist. One or more vulnerabilities are present and the aggressor is suspected of having the intent to exploit the school's assets.
Medium	5–6	Known aggressors or hazards that may be capable of causing loss of, or damage to, the school exist. One or more vulnerabilities may be present; however, the aggressors are not believed to have the intent to exploit the school's assets.
Medium Low	4	Known aggressors or hazards that may be capable of causing loss of, or damage to, the school exist. Aggressors have no intent to exploit the school's assets.
Low	2–3	Few or no aggressors or hazards exist. Their capability of causing damage to the school's assets is doubtful.
Very Low	1	No aggressors or hazards exist.

1.2.2.2 Consequences Assessment

Consequences are the adverse effects of a terrorist attack (or a hazard event) and reflect the nature and severity of losses sustained as a result of such an incident. The assessment of consequences of an attack on a school is a process of estimating the magnitude and type of damage or loss sustained as a result of that attack. Consequences can be expressed in terms of fatalities, injuries, property damage, economic losses, or other types of adverse effects such as psychological or social impacts. In the wake of some incidents, the immediate losses reverberate through the

society, triggering indirect or secondary losses, which can be far reaching and sometimes even more devastating than the direct losses. This is particularly true in cases of senseless violence against school children as evidenced by the Columbine and Beslan attacks (see Chapter 3). This primer focuses on the direct or immediate consequences—the effects on human health and safety and the direct physical effects of the attack on the targeted school and its various assets.



Consequences are the adverse effects of a terrorist attack (or a hazard event) and reflect the nature and severity of losses sustained as a result of such an incident.

Estimating consequences is by its very nature fraught with uncertainties. Although considerable knowledge base exists today about the effects of various types of weapons on people and structures, the accuracy in estimating consequences is still largely dependent on the situation and conditions at the target at the time of an incident. For example, an explosion or a fire outburst, or the release of airborne toxic chemical, whether accidental or intentional, will have different consequences depending on the physical circumstances, such as timing, occupancy, wind direction, air temperature, and various other factors.

Estimating direct consequences of an attack is accomplished by:

1. Identifying potential targets
2. Identifying the effects of weapons on people and buildings
3. Identifying physical and environmental conditions at the target
4. Quantifying the potential losses

Identifying Potential Targets

Potential school attackers typically choose their targets to maximize the impact of their attack (its consequences) and minimize the effort. Schools are usually perceived as easy targets where a successful attack might produce the greatest effect. This effect may involve anything from

massive casualties or physical destruction intended to induce psychological shock to symbolic acts that demonstrate a community's vulnerability and instill fear.

Potential consequences will depend on which specific school asset is most likely to be regarded as the primary target. They can be tangible, such as students and teachers, or building systems and equipment that support specific activities or operations, or intangible, such as a school's symbolic value to the community.

A school's core functions and processes define the nature of the target and, therefore, the magnitude of potential loss as a result of a particular attack type or hazard event. In terms of threats executed against a school, the potential consequences of a school's failure to protect the lives or health of its wards represent the most significant concern. Other functions range from institutional—such as educational and social functions—to the basic physical functions of a building (schools are often the designated emergency shelters). School functions can be, and have been disrupted in the past, but the consequences of such attacks are of a different order of magnitude than attacks in which the lives of children may be endangered.

By identifying core functions, the risk assessment can be focused on what a school does, how it does it, and how various threats can affect the wellbeing of occupants and the school's operations. This approach provides discussion topics and results in an accurate understanding of consequences.

Critical assets are identified in the next step. An asset is a resource of value requiring protection. An asset can be tangible (e.g., students, faculty, staff, school buildings, facilities, equipment, activities, operations, information) or intangible (e.g., processes or school's reputation). Recognizing that people are a school's most critical asset, answering the questions below will help identify and prioritize other physical assets that require protection.

- How many people may be injured or killed during a particular type of an attack or any other catastrophic incident that directly affects the school?
- What happens to occupants if a specific asset is lost or degraded? (Can primary services continue?)
- What is the impact on the school's functions and operations if one component in a system is lost or disabled?
- Who are faculty and staff whose loss would degrade, or seriously complicate the safety of students, faculty, and staff during an emergency?

First responders or the personnel responsible for shelter operations at a school that is a designated shelter for natural hazards should also be considered as critical assets.

- Does the school have any emergency backup systems?
- If so, can they be replaced quickly and at what costs if the school building systems' components are lost?

Effects of Weapons

Information on the effects of weapons may be readily available, because government agencies and many private organizations have long studied the effects of ballistic and explosive weapons as well as toxic and other substances on people and buildings. For example, a known quantity of explosive material detonated at a specific distance will produce air pressures sufficient to kill people and cause damage to structures. Similarly, information on the effects of exposure to various toxic substances or radiation is available and may be used in estimating the potential consequences of an attack with a specific type of weapon.

Identifying Conditions at the Target

The consequences of a hazardous event at or near the school are determined by the type of incident and the physical and environmental conditions at the target at the time of the event. A door left open will allow unimpeded access, just as the toxic release upwind of a nearby school will have different consequences during a windy day than during a still night. Physical conditions do not include the intrinsic characteristics of a school and its operations. These characteristics will be covered under the section on vulnerabilities. Physical and environmental conditions should be considered at their most disadvantageous state when analyzing and rating consequences, as in the following examples:

- **Timing** – Most schools operate on a fixed schedule, which means that attacks at different times of the day will have different consequences. An explosive attack during school hours can be catastrophic in terms of the number of students and staff who may be affected. In addition, schools may use different types of heating and cooling systems depending on the season, which may affect the consequences of a release of toxic substances.
- **Environment** – Wind speed and direction, air temperature, humidity, and other environmental conditions may affect the duration and severity of exposure to toxic substances in the air and aggravate the consequences of such an attack. Environmental conditions also affect the consequences of an explosive blast.

Quantifying Consequences

Rating of the gravity of consequences of an attack is difficult, because it requires judgments about relative values of various school assets. Which is worse—a small number of serious injuries or a large number of moderate injuries? Such questions cannot be answered with any objectivity and should be subject to a wider community and societal consensus.

The consequences rating should include the degree of debilitating effect that would be caused by the incapacity or destruction of the school's assets. The scale in Table 1-4 below uses the same type of numerical values used for threats and hazards to depict various levels of gravity of potential losses or consequences of an attack or hazard event. Each level describes the scope of potential fatalities and injuries and the degree of debilitating effects that would be caused by the damage to school assets. To put the consequences of an attack in the proper perspective, grave consequences such as fatalities and injuries must be rated on the same scale with potential building damages and other property losses. Although the losses associated with human assets will always be the primary criterion for assigning the consequences rating, other types of potential losses may raise or lower that rating.



The consequences rating should include the degree of debilitating effect that would be caused by the incapacity or destruction of the school's assets.

Table 1-4: Consequence Rating Scale

CONSEQUENCE RATING		
Very High	10	Loss or damage of the school's assets would have exceptionally grave consequences, such as extensive loss of life, widespread and severe injuries, or total loss of primary services for a long time. The consequences would have an exceptionally grave effect on the community's health and safety and public confidence. The school authorities have not taken steps to maintain continuity of operations to ensure that core functions would not be significantly affected by an event.
High	8–9	Loss or damage of the school's assets would have grave consequences, such as loss of life, severe injuries, or loss of primary services for a long time. The consequences would have a grave effect on the community's health and safety and public confidence. The school authorities have taken little or no action to maintain continuity of operations to ensure that core functions would not be significantly affected by an event.
Medium High	7	Loss or damage of the school's assets would have serious consequences, such as serious injuries or impairment of core functions for a long time. The consequences would have a serious effect on the community's health and safety and public confidence. The school authorities have taken minor steps to maintain continuity of operations to ensure that core functions would not be significantly affected by an event.
Medium	5–6	Loss or damage of the school's assets would have moderate to serious consequences, such as injuries or impairment of core functions for a considerable time. The consequences would have a moderate to serious effect on the community's health and safety and public confidence. The school authorities have taken some steps to maintain continuity of operations to ensure that core functions would not be significantly affected by an event.
Medium Low	4	Loss or damage of the school's assets would have moderate consequences, such as minor injuries or minor impairment of core functions and processes for a considerable time. The consequences would have a moderate effect on the community's health and safety and public confidence. The school authorities have taken moderate steps to maintain continuity of operations to ensure that core functions would not be significantly affected by an event.
Low	2–3	Loss or damage of the school's assets would have minor consequences, such as slight effects on core functions and processes for a short time, if at all. The consequences would have a minor effect on the community's health and safety and public confidence. The school authorities have taken reasonable steps to maintain continuity of operations to ensure that core functions would not be significantly affected by an event.
Very Low	1	Loss or damage of the school's assets would have negligible consequences and their effect on the community's health and safety and public confidence would be negligible. The school authorities have taken sufficient steps to maintain continuity of operations to ensure that core functions would not be significantly affected by an event.

1.2.2.3 Vulnerability Assessment

The consequences assessment estimates the magnitude of potential effects of an attack by looking at the attributes of the threat and surroundings at the time that a target is attacked, or exposed to a hazard event. In contrast, the vulnerability assessment evaluates the attributes of the target itself, as they constitute the characteristics inherent to the system (physical, organizational, or social) that may result in losses when the target is attacked. In cases of manmade hazards, vulnerabilities of a system are defined in technical and engineering terms, such as the capacity of a system to withstand and resist the forces acting on that system. For instance, two adjacent columns in a school building may be roughly the same distance from an explosion, but only one fails because it is struck by a fragment in a way that initiates collapse. In this sense, school vulnerabilities should be analyzed with respect to each structural element and its capacity to be overwhelmed by a substantial force.

The significance of vulnerabilities is underscored by the fact that aggressors frequently choose their targets in accordance with the verified weaknesses in those targets' defenses. The Oklahoma City bomber apparently chose the Alfred P. Murrah Federal building as his target because it was easier to approach than other targets that he had inspected. The terrorists who attacked the school in Beslan, Russia, are believed to have chosen an old building because its configuration made it easier to barricade and defend against a counterattack than a modern school building. The vulnerability of the target may not be the most important consideration for an attack, but glaring weaknesses in a school's organization, layout, and security arrangements may attract attention and act as an invitation to belligerence. A vulnerability assessment is particularly useful for identifying single point vulnerabilities at critical nodes or locations where one incident caused by a threat or hazard can affect more than one critical asset or both the primary and backup capabilities of a single system.

Vulnerability estimates are usually subject to lower levels of uncertainty than threats and consequences. Because vulnerability measures the likelihood that an attack of a specific type and magnitude will be successful against a target, it can be carefully studied and evaluated, and estimates are frequently readily available. For example, engineering and military risk analyses evaluating the effects of explosive blasts on structures or personnel can be used to identify specific vulnerabilities to these types of threats.

Three main aspects of a school's vulnerability must be taken into account:

- Structural
- Nonstructural
- Organizational

Structural Vulnerability

Structural vulnerability is related to potential damage to structural components of a school building. These components include foundations, bearing walls, columns and beams, staircases, floors and roof decks, or other types of structural components that help support the building.

The level of vulnerability of these components depends on the following factors:

- The architectural and structural form or configuration of a school building
- The level to which the design of the structural system has addressed the threat/hazard forces that impact that system



Structural vulnerability is related to potential damage to structural components of a school building.

- The quality of building materials, construction, and maintenance

Nonstructural Vulnerability

Nonstructural elements are much more vulnerable to explosive blast than the building structure. Nonstructural elements are attached to a building or building system, but are not part of the main load-resisting structural system of the building. They are easily damaged and costly to repair or replace. In most modern buildings, the nonstructural components account for 60 to 80 percent of the value of the building. In cases of explosive blast, many nonstructural components may be exposed to forces they were not designed to resist. Among others, interior walls, mechanical systems, fire protection systems, parapets, appendages, ornamentations, veneer, cladding systems, suspended ceilings, electrical components, and light fixtures cannot be designed and constructed to the same standards of blast and penetration resistance as the structural elements. The failure of these systems can significantly disrupt the functions and operation of the building and substantially increase the risk of death and injury for the occupants.

Most modern schools use centralized air and ventilation systems as well as municipal lifeline systems, all of which are extremely vulnerable to attacks with CBR weapons. Attacks on schools using weapons that do not primarily target the building structure, such as CBR devices could

seriously impair the safety of school occupants, even when the facilities do not sustain significant structural damage. The effects of attacks on nonstructural building components and equipment can be as dangerous and as disruptive to occupant safety, as any structural damage.



Nonstructural elements are much more vulnerable to explosive blast than the building structure.

Organizational Vulnerabilities

Organizational vulnerabilities include characteristics of school spatial organization (layout and building configuration), as well as operational and procedural routines that may be exploited by the attackers. Most schools have emergency operation plans (also be known as a crisis management plans), but not all of them provide organizational alternatives in the event of an attack. The spatial organization of a school's activities and their inter-relationships frequently determine the extent to which the school facilities are vulnerable to various types of attacks. The critical nature of spatial organization represents a separate category of vulnerabilities that needs careful attention.

Evacuation or rescue of students and staff under attack is a measure of last resort, which may be necessary in extreme situations. Many different situations may require safe escape routes and routines, but the process of evacuation itself may constitute a vulnerability that potential attackers may use to their advantage as in both the Columbine and Jonesboro shooting attacks where the schools' pre-planned drills moved students outside of the school where they were exposed to the aggressors (see Chapter 3).

The School Vulnerability Assessment Checklist provided in Appendix F is based on a checklist developed by the U.S. Department of Veterans Affairs and the National Clearinghouse for Educational Facilities and compiles many best practices, based upon technologies and scientific research, to consider during the design of a new building or an assessment of an existing school building. The checklist allows a consistent security evaluation of designs at various levels. It can be used as a screening tool for an initial vulnerability assessment or be used by subject matter experts for a comprehensive vulnerability assessment of existing school buildings.

The assessment of vulnerabilities of a school building should be done within the context of the defined threats and the school's assets or potential targets. That is, each element of the school's core functions and critical assets should be analyzed for vulnerabilities to each threat/hazard and a vulnerability rating should be assigned. The same type of numerical scale used in the threat and consequences assessments can be used for the vulnerability assessment, as presented in Table 1-5.



Organizational vulnerabilities include characteristics of school spatial organization as well as operational and procedural routines.

Table 1-5: Vulnerability Rating Scale

VULNERABILITY RATING		
Very High	10	One or more major weaknesses have been identified that make the school's assets extremely susceptible to an aggressor or hazard.
High	8–9	One or more significant weaknesses have been identified that make the school's assets highly susceptible to an aggressor or hazard.
Medium High	7	An important weakness has been identified that makes the school's assets very susceptible to an aggressor or hazard.
Medium	5–6	A weakness has been identified that makes the school's assets fairly susceptible to an aggressor or hazard.
Medium Low	4	A weakness has been identified that makes the school's assets somewhat susceptible to an aggressor or hazard.
Low	2–3	A minor weakness has been identified that slightly increases the susceptibility of the school's assets to an aggressor or hazard.
Very Low	1	No weaknesses exist.

1.2.2.4 Risk Analysis

Risk is the potential for a loss of or damage to an asset. It is determined based upon the level of potential consequences related to the given threat and the level of vulnerability of the targeted assets to that threat. Risk is based on the likelihood or probability of the attack or hazard event occurring and the probability that a successful attack or event will cause the maximum potential losses. Risk assessment analyzes the potential for occurrence of each applicable threat/hazard for each asset.

The potential losses are determined based on potential consequences and vulnerabilities of the asset. Thus, a very high likelihood of occurrence with very small consequences may have a low risk rating and may warrant only simple low-cost mitigation measures, but a very low likelihood of occurrence with very grave consequences will

have a high risk rating that warrants more costly and complex mitigation measures. The risk assessment provides engineers, architects, and school administrators with a relative risk profile that defines specific assets that are at the greatest risk from specific threats. Chapters 3, 4, and 5 explore school vulnerabilities to particular threats and recommend cost-effective protective measures to address those vulnerabilities.



Risk is the potential for a loss of or damage to an asset.

Numerous methodologies and techniques exist for conducting a risk assessment. One approach is to assemble the results of the threat assessment, consequences assessment, and vulnerability assessment, and to determine a numeric value of risk for each asset and threat/hazard pair in accordance with the following formula:

$$\text{Risk} = \text{Threat Rating} \times \text{Consequences Rating} \times \text{Vulnerability Rating}$$

Table 1-6 below provides a numerical scale to apply various levels of risk of potential losses or consequences of an attack or hazard event.

Table 1-6: Risk Rating Scale

Vulnerability		
Very High	≥ 261	The potential for loss or damage of the school's assets is so great as to expect exceptionally grave consequences, such as extensive loss of life, widespread severe injuries, or total loss of primary services and core functions and processes.
High	201–260	The potential for loss or damage of the school's assets is so great as to expect grave consequences, such as loss of life, severe injuries, loss of primary services, or major loss of core functions and processes for an extended time.
Medium High	141–200	The potential for loss or damage of the school's assets is such as to expect serious consequences, such as serious injuries or impairment of core functions and processes for an extended time.
Medium	101–140	The potential for loss or damage of the school's assets is such as to expect serious consequences, such as injuries or impairment of core functions and processes.
Medium Low	61–100	The potential for loss or damage of the school's assets is such as to expect only moderate consequences, such as minor injuries or minor impairment of core functions and processes.
Low	31–60	The potential for loss or damage of the school's assets is such as to expect only minor consequences or impacts, such as a slight impairment of core functions and processes for a short time.
Very Low	1–30	The potential for loss or damage of the school's assets is so low that the consequences or impacts would be negligible.

As a minimum, mitigation measures to reduce risk and create an acceptable level of protection should be considered for those critical assets determined to be at highest risk.

Risk assessment is an initial step in the process of managing the risks to which a school may be exposed. This process considers many more issues and requires the cooperation of school officials and other stakeholders.

1.3 Risk Reduction

Risks are quantified and prioritized to make decisions about how best to manage them. Risk reduction requires that protective policies be enforced and protective actions be taken before an incident. For all practical purposes, managing threats is outside the purview of school authorities, who must rely on law enforcement and other government agencies for help. Consequently, the risk reduction efforts of school authorities must focus on activities aimed at reducing the vulnerabilities and minimizing the consequences.



Risks are quantified and prioritized to make decisions about how best to manage them.

Most protective measures are designed to alleviate a particular vulnerability to a specific threat or hazard, or to help reduce the potential consequences, as discussed in later chapters. However, many of these measures designed to address particular vulnerabilities may have adverse effects with respect to another type of threat or

hazard. To identify, select, and implement the most appropriate protective measures, the risk reduction objectives and merits of each potential protective measure must be evaluated against each identified threat or hazard. Evaluating the effectiveness of a particular measure, whether regulatory or technical, requires comprehensive technical, policy, and financial expertise combined with a thorough knowledge of the educational environment and its requirements.

1.3.1 Evaluating Protective Measures

The selection and implementation of protective measures to achieve an acceptable level of protection at an acceptable cost is perhaps the most important component of the risk management process. Because protecting against the entire range of possible threats is cost prohibitive, developing a realistic prioritization of risk reduction objectives and measures that respond to these objectives is important. When evaluating protective measures, consider the following factors:

- The results of the risk assessment, including consequences and vulnerabilities
- The costs of the protective measures (both initial installation and recurring for operation and maintenance)
- The value (in terms of life safety and protection) of risk reduction for the school and community as a whole
- The deterrence or preventive value of the protective measures
- The expected lifespan of the protective measures

To evaluate protective measures, decisionmakers should first reassess the potential effects of each measure on the vulnerabilities and consequences for each threat and/or hazard under consideration. Many protective measures affect vulnerabilities and consequences for multiple threats and hazards, some of them adversely, so a careful cross-examination of these conflicting effects is important. After evaluating the effects of the recommended protective measures on the risk rating for each attack type, costs of each measure should be estimated using a variety of economic tools and cost-estimating resources. In some cases, conducting a benefit-cost analysis may be necessary to determine which protective measures will produce the greatest reduction of risk at an acceptable cost.

The deterrent or preventive value of a protective measure is difficult to quantify but should not be underestimated. Deterrence, in the case of terrorism, may also have a secondary impact in that, once a school building is “hardened,” a terrorist may turn to a less protected building, changing the likelihood of an attack for both targets. For example, the Murrah Federal Building in Oklahoma City became a target after Timothy McVeigh was deterred from attacking the FBI building, because getting the attack vehicle close to that target was too difficult. He was able to park immediately adjacent to the Murrah Federal Building and successfully target the Bureau of Alcohol, Tobacco, and Firearms.

All these factors should be considered when calculating the value of protective measures, and weighing their value against their cost. Ideally, sufficient resources would be available to achieve a desired level of protection, but this is not always the case. Consequently, every school district should identify or designate an appropriate authority to make the risk-related decisions on behalf of the school.

1.3.2 Implementing Protective Measures

Risk reduction or mitigation activities focus on minimizing the effects of an attack or hazard event, i.e., minimizing the probability that such an attack or event will cause casualties, destruction, or disruption. Determining the most appropriate protective measures is not an intuitive process. It is best undertaken as a continuation of the risk assessment process to avoid the implementation of risk reduction measures that may not be adequate for the desired level of protection, or may not address the priority concerns or vulnerabilities. A detailed risk assessment and evaluation of risk reduction measures will facilitate the design and implementation of effective protective measures that can be integrated into the normal operations and activities of educational facilities at a reasonable cost.



Risk reduction or mitigation activities focus on minimizing the effects of an attack or hazard event.

The implementation of protective measures usually takes place in one of three different situations:

- As a result of increased focus on risk reduction following a serious incident. This heightened level of awareness provides an opportunity and a favorable social environment for implementing protective measures, for which adequate support, especially funding, might otherwise be difficult to mobilize.
- The construction of new educational facilities, which allows new measures to be integrated into the plans and designs from the very beginning. This is the most cost-efficient approach.
- The implementation of protective measures into an existing environment. This is often the most challenging situation because of the frequently insurmountable technical, logistical, or cost constraints.

To facilitate the implementation of protective measures, decisionmakers are encouraged to approach mitigation both as a comprehensive process, encompassing and integrating diverse social, educational, logistical, and technical measures, and as a continuing long-term process that reinforces and reinvents itself based on experience. Specifically, school security protective initiatives should not be isolated from the community's security and hazard risk management activities, but should be part of an integrated strategy for risk reduction. Considering the scarcity of resources, school authorities should make a compelling case to the community's decisionmakers using the methods of risk assessment described in this primer to show that the protection of schools protects the most vulnerable and most precious of a community's resources.

1.3.3 Preparing School Safety Emergency Plans

DHS has designated the U.S. Department of Education (ED) as the lead agency for school-related security. The ED has published a guide, *Practical Information on Crisis Planning: A Guide for Schools and Communities* (January 2007) that is intended to provide schools, districts, and communities with the critical concepts and components of good crisis planning, stimulate thinking about the crisis preparedness process, and provide examples of best practices. Additional general information is available from the National Advisory Committee on Children and Terrorism, as well as information specifically covering bioterrorism issues in conjunction with the Centers for Disease Control and Prevention (CDC). Other school health and safety issues are covered by various tools and publications of the CDC's Division of Adolescent and School Health.

The ED recommends each school safety emergency plan address the four major areas listed below:

■ **Mitigation**

- Conduct an assessment of each school building. Identify those factors that put the building, students, faculty, and staff at greater risk, such as proximity to rail tracks that regularly transport hazardous materials or to facilities that produce highly toxic material or house propane gas tanks, and develop a plan for reducing the risk. This plan could address evacuating students away from these areas in times of crisis and repositioning propane tanks or other hazardous materials away from school buildings.
- Work with businesses and factories in close proximity to the school to ensure that the school's emergency plan is coordinated with their emergency plans.
- Ensure that a process is in place for controlling access and egress to the school. Require all persons who do not have authority to be in the school to sign in.
- Review traffic patterns, and where possible, keep cars, buses, and trucks away from school buildings.
- Review landscaping, and ensure that buildings are not obscured by overgrowth of bushes or shrubs where contraband can be placed or persons can hide.

■ **Preparedness**

- Have site and floor plans for each school building readily available and ensure they are shared with first responders and agencies responsible for emergency preparedness.
- Establish multiple evacuation routes and rallying points. First or second evacuation site options may be blocked or unavailable at the time of the crisis.
- Practice responding to crisis on a regular basis.
- Ensure a process is established for both internal and external communications during a crisis.
- Inspect equipment regularly to ensure it will operate properly during crisis situations.
- Create a plan for discharging students. Remember that, during a crisis, many parents and guardians may not be able to get to the school to pick up their child. Make sure the school has a secondary contact person and contact information readily available for every student.
- Develop a plan for communicating information to parents and for quelling rumors. Cultivate relationships with the media ahead

of time, and identify a Public Information Officer to communicate with the media and the community during a crisis.

- Work with law enforcement officials and emergency preparedness agencies on a strategy for coordination to include as part of the school emergency plan.
- Develop a command structure for responding to a crisis. The roles and responsibilities for educators, law enforcement and fire officials, and other first responders in responding to different types of crisis need to be developed, coordinated, reviewed, and approved.
- **Response**
 - Identify the type of crisis and determine the appropriate response.
 - Maintain communications among all relevant staff.
- **Recovery**
 - Return to the business of teaching and learning as soon as possible.
 - Identify and approve a team of credentialed and adequately trained mental health workers to provide mental health services to faculty and students after a crisis. Understand that recovery takes place over time and that the services of this team may be needed over an extended period.
 - Notify parents on actions that the school intends to take to help students recover from the crisis.

Every school should have a school safety emergency plan, as described above, developed in partnership with public safety agencies, including law enforcement, fire, public health, mental health, and local emergency preparedness agencies. The plan should consider risks like fire, and natural and manmade disasters. A school's plan should be tailored to address the unique circumstances and needs of the individual school, and should be coordinated and integrated with community plans and the plans of local emergency preparedness agencies.

These plans should consider all identified threats/hazards and attack scenarios and the associated procedures for communicating instructions to building occupants related to emergency evacuations or other protective activities. They should also identify the most suitable shelter-in-place areas (if they exist) and identify appropriate use and selection of personal protective equipment (e.g., clothing, gloves, respirators). Individuals developing emergency plans and procedures should recognize that fundamental differences between different emergency situations may require different instructions and response routines. The plans should be as comprehensive as possible and shared with relevant coordinating agencies but not with the general public. When appropriately developed, these plans,

policies, and procedures can have a major impact on school occupant survivability in the event of an attack or exposure to a technological hazard.

Staff training, particularly for those with specific responsibilities during an event, is essential to an effective emergency response. Holding regularly scheduled practice drills, similar to the common fire drill, allows for plan testing, as well as student and key staff rehearsal of the plan, and increases the likelihood for a successful response in an actual event. School officials should ensure that training is provided to staff that operate and maintain the school's critical systems.

1.4 Response

Each school day, more than 50 million students are entrusted to the care of the public school system and many private schools. On most days, these schools are safe havens for teaching and learning, but in an emergency, school personnel may need to serve as first responders for natural hazard events like tornadoes, earthquakes, or floods, or manmade hazards and accidents like toxic spills. Increasingly, the critical incidents that may threaten the safety of schools include intentional attacks on students, faculty, or school property.

The response to terrorist or other types of attacks and similar crises usually involves first responders (the police and other law enforcement agencies, the fire department, and ambulances) and many others, as well as scores of onlookers, media, and, in the case of schools, concerned parents and relatives that gather around the scene. The more serious the incident, the more serious is the task of organizing the response and controlling the situation. The chaotic events that surrounded the terrorist attack on a school in Beslan, Russia, (see Chapter 3) showed very clearly the pitfalls of an uncoordinated response to a critical incident.

Professional responders involved in response activities to large-scale emergencies now use an Incident Command System (ICS) to organize and coordinate the response. ICS is part of a National Incident Management System that integrates existing best practices into a consistent, nationwide approach to domestic incident management applicable at all jurisdictional levels and across functional disciplines. ICS defines the operating characteristics, interactive management components, and structure of incident management and emergency response organizations engaged in an incident. The structure of ICS facilitates activities in five major functional areas: command, operations, planning, logistics, and finance administration. ICS is also flexible and scalable allowing for functional areas to be added as necessary and terminated when no longer necessary.

ICS allows school personnel and community responders to adopt an integrated organizational structure that matches the complexities and demands of the incidents without being hindered by jurisdictional boundaries. Although school-based incidents most likely will not need many of the standard ICS facilities common to large disasters, the flexibility of ICS makes it a very cost-effective and efficient management approach for both small and large incidents.

1.5 Decisionmaking

Some of the most important aspects of risk management are the decisions that have to be made about the types of risks to which a school may be exposed and the prioritization of those risks according to a set of common criteria. The questions that are usually asked include:

- Which threats are the most immediate and most serious?
- Which ones could have the most serious consequences?
- To what extent would the identified vulnerabilities contribute to the losses, were the attack to take place?
- Are these risks serious enough to require action? If they are, what action would be the most effective in reducing that risk?

All such decisions are fraught with uncertainties, i.e., they require decisionmakers to exercise judgments that are not based on any reliable set of data or agreed values.

1.5.1 Uncertainties and Value Judgments

Uncertainties affect the risk management from the very start. To many, the risk assessment process may appear to be a neutral academic exercise, until such a time when decisions have to be made about the level of acceptable risk, or when priorities in the allocation of limited resources for school protection have to be set. According to RAND Corporation's Center for Terrorism Risk Management Policy (Willis and Kelly 2005), two important sources of uncertainty exist in assessing the risks. The first one reflects imprecise methods for estimating the likelihood of occurrence of any particular type of attack (threat) or the scope of consequences that may result from such an attack. The second stems from a lack of any universally accepted set of criteria by which to compare and value the consequences. Table 1-4 is but one attempt to map the consequences according to their relative magnitude from a community perspective. The obvious difficulty arises when determining the relative gravity of consequences of an incident with a large number of moderately wounded individuals compared with an incident that resulted in a few serious injuries or extensive physical damage. No guidelines or criteria explain what society should value more, which makes it all the more

important for the risk assessment process to address these uncertainties in an open discussion with all the stakeholders.

1.5.2 Acceptable Level of Risk

The daily lives of individuals and communities are full of risks of various types and severity. The decisions about these risks are made routinely based on experience. People do not perform a risk assessment before crossing a busy street, but they do stop to think when faced with unfamiliar risks. They also stop to think when the consequences may be too grave to ignore. In such situations, people consider the likelihood that a certain event will take place and cause feared consequences. The likelihood of a serious automobile accident is usually considered miniscule and, despite potentially grave consequences, routinely dismissed by millions of drivers on a daily basis. These decisions are a product of a conscious trade-off. The risks are usually deemed tolerable when compared with the cost and inconvenience of not using an automobile. More to the point, one other significant factor influences these and similar decisions to accept the risks—the confidence of decisionmakers in the risk reduction activities they usually employ. The drivers consciously drive on the designated side of the road, strap on their seat belts, and observe the traffic rules. That is, the decisionmakers are more likely to find the risks acceptable, in spite of potentially horrifying consequences, if the likelihood of the event is small, and sufficient and reasonable precautions, or protective measures, have been put in place.

Such decisionmaking is similar to what school administrators face when considering security threats and manmade hazards. They are no different than the decisions made daily by individuals about their own lives, except that they now affect the lives of others, frequently entire communities. The responsibility to protect the most precious resource of a society—its children—may weigh differently on individual aspects of the risk, but ultimately, decisions have to be made about the most appropriate level of protection. That level of protection is defined by the acceptable level of risk and by the selection and implementation of the most effective protective measures.

1.5.3 Cost Estimation

A general spectrum of protective measures ranging from the least protective and least costly to the most protective and most costly are provided in Figures 1-4 and 1-5. These protective measures are arranged by layers of defense (described in Chapter 2): the first layer is outside the perimeter of the school, the second layer is between the perimeter and the building, and the third layer generally refers to the school building itself. Examples of protective measures are provided for each layer.

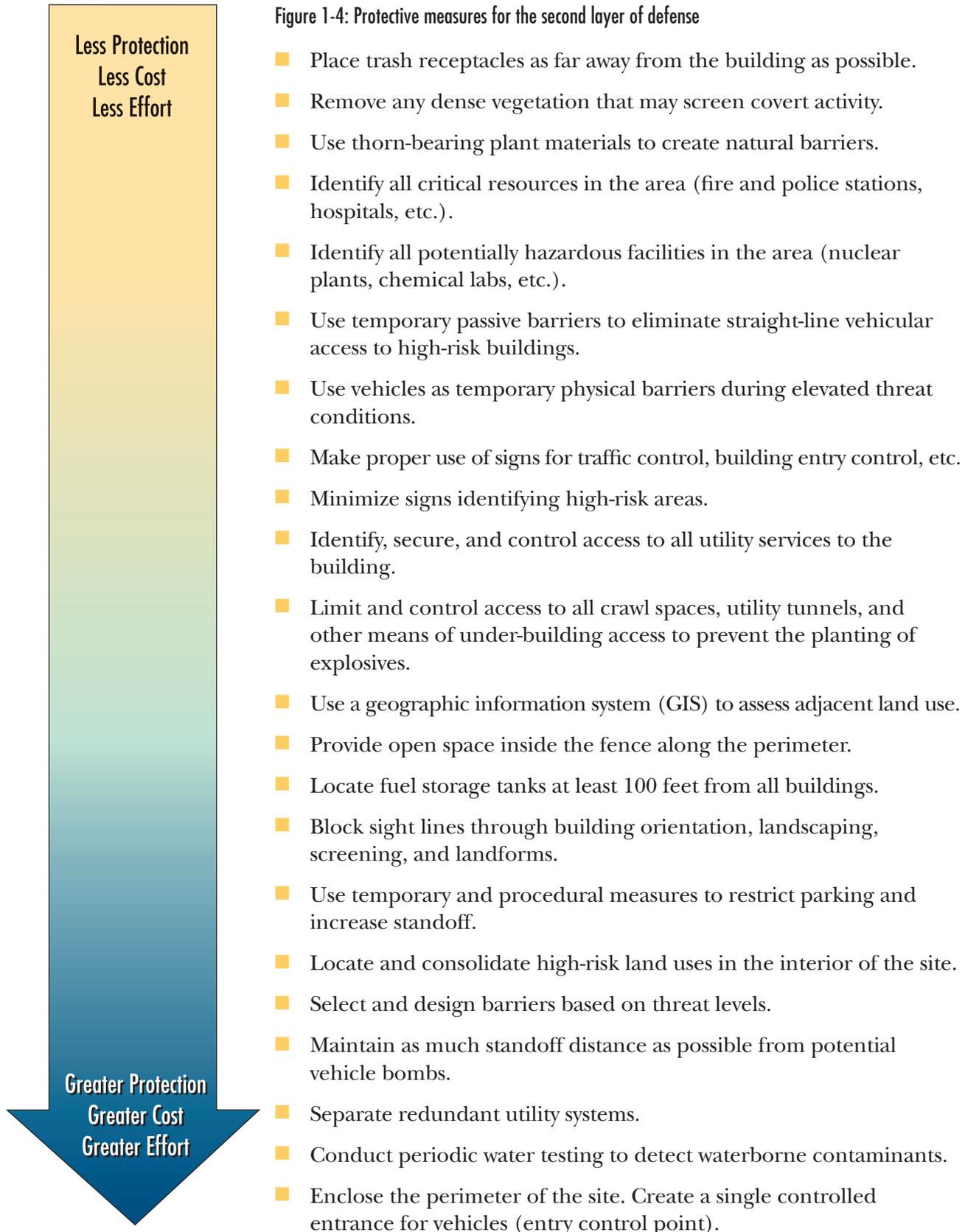


Figure 1-4 : Protective measures for the second layer of defense (cont.)

- Establish law enforcement or security force presence.
- Install quick connects for portable utility backup systems.
- Install security lighting.
- Install closed-circuit television (CCTV) cameras.
- Mount all equipment to resist forces in any direction.
- Include security and protection measures in the calculation of land area requirements.
- Design and construct parking to provide adequate standoff for vehicle bombs.
- Position buildings to permit occupants and security personnel to monitor the site.
- Site the building at an appropriate distance from to potential threats or hazards.
- Locate critical building components away from the main entrance, vehicle circulation, parking, or maintenance area. Harden as appropriate.
- Provide a site-wide public address system and emergency call boxes at readily identified locations.
- Prohibit parking beneath or within a building.
- Design and construct access points at an angle to oncoming streets.
- Designate entry points for commercial and delivery vehicles away from high-risk areas.
- In urban areas, push the perimeter out to the edge of the sidewalk by means of bollards, planters, and other obstacles. For better standoff, push the line farther outward by restricting or eliminating parking along the curb, eliminating loading zones, or closing streets.
- Provide intrusion detection sensors for all utility services to the building.
- Provide redundant utility systems to support security, life safety, and rescue functions.
- Conceal and/or harden incoming utility systems.
- Install active vehicle crash barriers.

Less Protection
Less Cost
Less Effort

Greater Protection
Greater Cost
Greater Effort

Less Protection
Less Cost
Less Effort

Greater Protection
Greater Cost
Greater Effort

Figure 1-5: Protective measures for the third layer of defense

- Install active vehicle crash barriers. Ensure that exterior doors into inhabited areas open outward. Ensure emergency exit doors only facilitate exiting.
- Secure roof access hatches from the interior. Prevent public access to building roofs.
- Restrict access to building operation systems.
- Conduct periodic training of heating, ventilation, and air-conditioning (HVAC) operations and maintenance staff.
- Evaluate HVAC control options.
- Install empty conduits for future security control equipment during initial construction or major renovation.
- Do not mount plumbing, electrical fixtures, or utility lines on the inside of exterior walls.
- Establish emergency plans, policies, and procedures.
- Establish written plans for evacuation and sheltering in place.
- Illuminate building access points.
- Restrict access to building information.
- Secure HVAC intakes and mechanical rooms.
- Limit the number of doors used for normal entry/egress.
- Lock all utility access openings.
- Provide emergency power for emergency lighting in restrooms, egress routes, and any meeting room without windows.
- Install an internal public address system.
- Stagger interior doors and offset interior and exterior doors.
- Eliminate hiding places.
- Install a second and separate telephone service.
- Install radio telemetry distributed antennas throughout the facility.
- Use a badge identification system for building access.
- Install a CCTV surveillance system.
- Install an electronic security alarm system.
- Install rapid response and isolation features into HVAC systems.

Figure 1-5: Protective measures for the third layer of defense (cont.)

- Use interior barriers to differentiate levels of security.
- Locate utility systems away from likely areas of potential attack.
- Install call buttons at key public contact areas.
- Install emergency and normal electric equipment at different locations.
- Avoid exposed structural elements.
- Reinforce foyer walks.
- Use architectural features to deny contact with exposed primary vertical load members.
- Isolate lobbies, mailrooms, loading docks, and storage areas.
- Locate stairwells remotely. Do not discharge stairs into lobbies, parking, or loading areas.
- Elevate HVAC fresh-air intakes.
- Create “shelter-in-place” rooms or areas.
- Separate HVAC zones. Eliminate leaks and increase building air tightness.
- Install blast-resistant doors or steel doors with steel frames.
- Physically separate unsecured areas from the main building.
- Install HVAC exhausting and purging systems.
- Connect interior non-load-bearing walls to structure with non-rigid connections.
- Use structural design techniques to resist progressive collapse.
- Treat exterior shear walls as primary structures.
- Orient glazing perpendicular to the primary façade facing uncontrolled vehicle approaches.
- Use reinforced concrete wall systems in lieu of masonry or curtain walls.
- Ensure active fire system is protected from single-point failure in case of blast event.
- Install a backup control center.
- Avoid eaves and overhangs or harden to withstand blast effects.
- Establish ground floor elevation four feet above grade.
- Avoid re-entrant corners as the building exterior.

Less Protection
Less Cost
Less Effort

Greater Protection
Greater Cost
Greater Effort

Site Design for Security



In this chapter:

This chapter discusses comprehensive architectural and engineering design considerations (protective measures) for the school site, from the property line to the school building, including land use, site planning, standoff distance, controlled access zones, entry control and vehicular access, signage, parking, loading docks, and service access.

2.1 Introduction

This chapter discusses comprehensive architectural and engineering design considerations (protective measures) for the school site, from the property line to the school building, including land use, site planning, standoff distance, controlled access zones, entry control and vehicular access, signage, parking, loading docks, and service access. The intent of this guidance is to integrate security requirements into a comprehensive approach to design for the purpose of achieving balance among objectives such as reducing risk, facilitating proper school building function, addressing aesthetics and matching architecture, creating a school environment conducive to learning, and hardening of physical structures for added security.



The design community must work closely with school districts and school administrators to reach the optimal balance between considerations.

The design community must work closely with school districts and school administrators to reach the optimal balance between these considerations. Thus, coordination within the design team is critical. Many school protection objectives can be achieved during the early stages of

the design process when protective measures are the least costly and most easily implemented. Planners, architects, and landscape designers play an important role in implementing and integrating crucial protective measures into the design process, from site selection, orientation of school buildings on the site, to vehicle access, control points, physical barriers, landscaping, parking, and protection of utilities.

The nature of any threat is always changing. Although indications of potential future threats may be scarce during the design stage, consideration should be given to accommodating enhanced protection measures in response to future threats that may emerge. School protection objectives must be balanced with other design objectives, such as the efficient use of land and resources, and must also take into account existing physical, programmatic, and fiscal constraints.

2.2 School Sites

Site design can play a major role in guarding against attacks that are carried out by inside or outside perpetrators who, for whatever reasons, target a school and its occupants. The major threats faced by schools are various types of shooters, small bombs that may be carried into the school by one or two people, and the possible use of CBR agents as a direct means of attack or an indirect collateral threat.

Table 1-3 in Chapter 1 suggests a nominal school threat assessment. The threat ratings range from 1 (very low) for a stationary vehicle bomb and hydrogen sulfide bomb, 2 (low) for an attack with small arms, to 3 (low) for forced entry at night to damage school property and electronic attack of school computer records. A measure of these threat ratings may be gained from national records of the school year 2006–2007. In that year, 27 homicides and 8 suicides of school-age youths (ages 5–18) occurred at schools. Of these, nine persons were victims of five active shooter attacks in schools. One of these attacks killed five people, while the others each killed one person. In three of these attacks the perpetrator was an adult: the other attacks involved a student. During this school year, the total national enrollment of students was approximately 49 million.



In addition to the design of specific security-related measures, site design for security involves the integration of general planning tasks, such as building placement and parking and site infrastructure planning, with security needs.

In addition to the design of specific security-related measures, site design for security involves the integration of general planning tasks, such as building placement and parking and site infrastructure planning, with security needs. In this publication, security measures are discussed as they apply to existing facilities, but the measures can also be used in the design and evaluation of a proposed site and school design.

2.2.1 Suburban/Rural School Sites

As a result of the massive expansion of the suburbs of large cities following World War II, and the continued existence of small towns, most U.S. schools are located on suburban/rural sites.

Although smaller schools may have only one building, larger schools are usually organized as a campus, with a number of separate buildings connected by open or closed walkways. Figures 2-1 to 2-4 show a campus-type grades 8–12 high school. This school opened in 1898 and moved to its present location in 1919. Figures 2-2 and 2-3 show the theater and the administration building and entry tower, which date back to 1919. Figure 2-4 shows part of the 1964 campus, with one-story buildings arranged around a quadrangle.

Figure 2-1:
Campus-style grades 8–12
high school

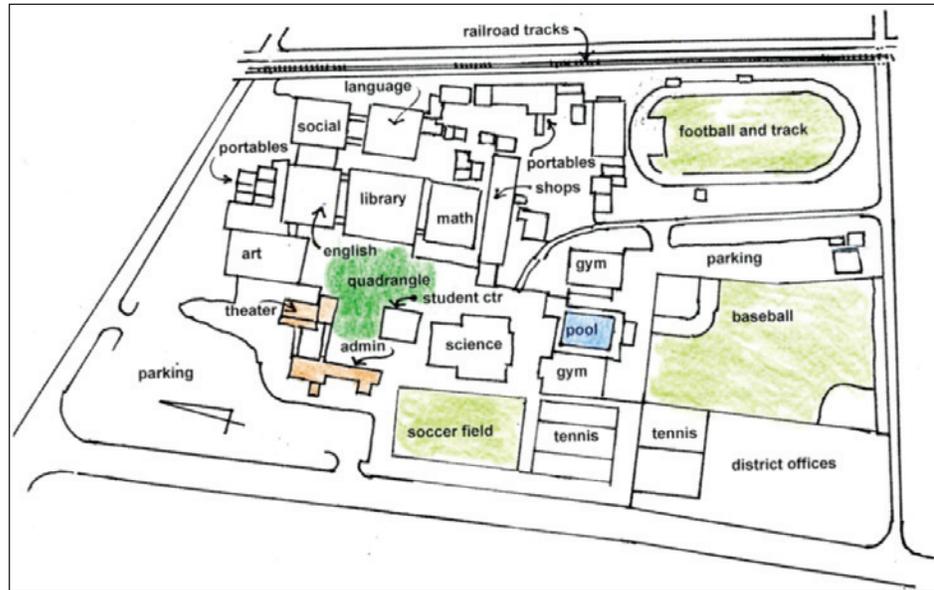


Figure 2-2:
Theatre building on the school
campus



Figure 2-3:
The administration building
and entrance tower on the
school campus





Figure 2-4:
School campus buildings from
the 1960s

Figures 2-5 to 2-7 show a campus-type grades 8–12 high school in the same school district. This school opened in 1964 and consists of a number of one-story buildings, each housing a different discipline, connected with open walkways, many also arranged around a quadrangle. Figure 2-6 shows the entry to the school and Figure 2-7 shows a typical campus building from the main street that borders the campus. Both schools provide ample parking for staff, students, and visitors and spacious on-site playing fields.

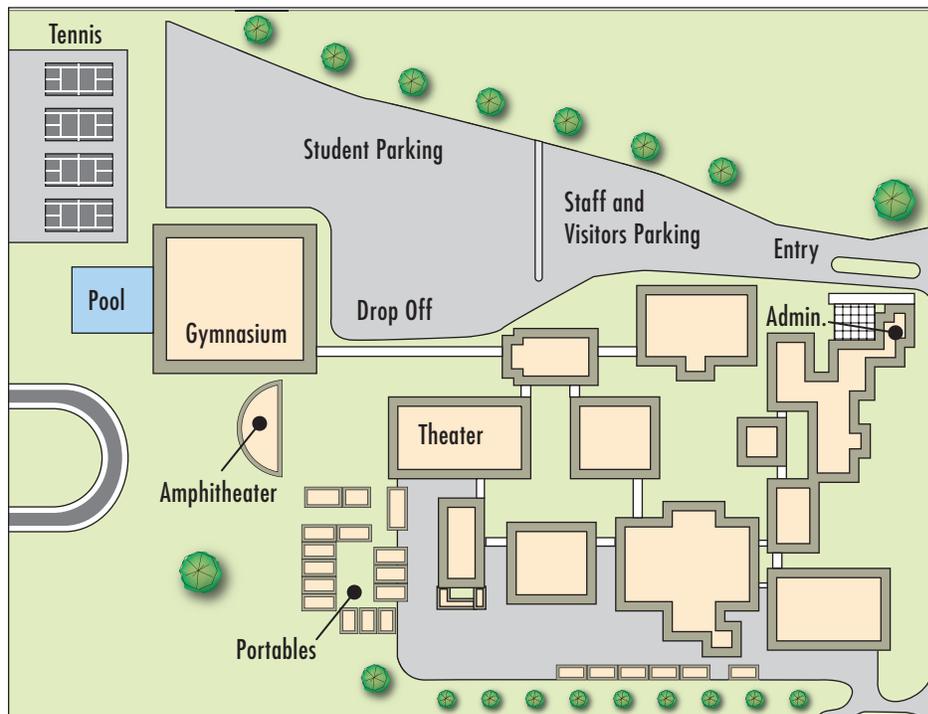


Figure 2-5:
High school campus from
1960s

Figure 2-6: Main entrance



Figure 2-7:
View from the main street



2.2.2 Urban School Sites

Urban schools are seldom placed in the central business district, but rather are located to serve the inner-residential areas, often at the site of high-density housing. For several decades, the inner-city populations have been fairly static or even reduced, and population growth has been concentrated in ever-expanding suburbs. Thus, new school construction has been largely a suburban phenomenon and, as a result, inner-city schools tend to be much older buildings. As an example, of the 16 high schools located in San Francisco, 12 are over 40 years old. The oldest was built in 1910, and three more were constructed in 1924. The three newest were built in 1995, 2000, and 2009.

City land is expensive, and so inner-city school sites are very small compared to their suburban counterparts. Buildings typically have two or three stories, and roofs often serve as playgrounds. Some older schools are located adjacent to public parks, which helps in providing a play area for the school population.

Figure 2-8 shows an urban high school constructed in 1924, and recently beautifully rehabilitated, that occupies a city block and is surrounded on all four sides by major streets. Figure 2-9 shows the site plan of this school and specifically how close the school is in relation to the public sidewalks and traffic. Figure 2-10 shows the restored entrance to the school and courtyard.



Figure 2-8:
An urban high school,
constructed 1924; note the
classrooms adjacent to the
public sidewalk and vehicle
traffic

Figure 2-9:
Site plan of the high school shown in Figure 2-8; note traffic on all four sides with interior courtyard and classrooms adjacent to a public sidewalk

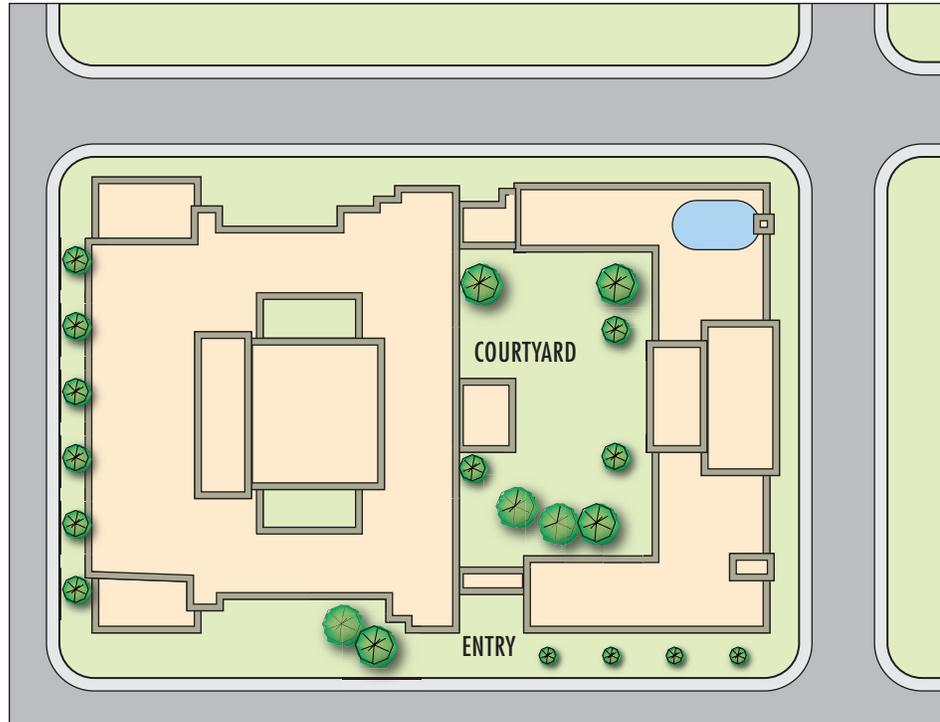


Figure 2-10:
Restored architecture of the school entrance and courtyard from the main street



Figure 2-11 shows a school located in an urban residential neighborhood of single-family homes and modest size multi-family apartments. Many older schools—constructed prior to World War II—were designed as important community symbols and are of a high architectural quality.



Figure 2-11:
Urban high school in inner-city residential neighborhood of single-family houses

Figure 2-12 shows an inner-city school in a dense residential and commercial location that is also across the street from a large public park. The school entrance tower is a significant neighborhood symbol. The school was founded in 1897 and the present building, constructed in 1924, houses a museum showing the evolution of the school over the last 100 years.



Figure 2-12:
Urban high school as an important neighborhood symbol, constructed in 1924

2.2.3 Security Implications of Site Characteristics

The following are some of the site characteristics that may affect the vulnerability of a school building to blast and CBR attacks:

- School footprint relative to total land available
- Existing or proposed location relative to the site perimeter and adjacent land uses, and the available distance between the defended perimeter and improved areas offsite
- Overall size and number of the buildings to be placed onsite
- Massing and placement of school buildings that may impact views, sight lines, and screening
- Access via foot, road, rail, water, and air
- Presence of natural physical barriers, such as water features, dense vegetation, and terrain, that could provide access control or shielding, or suitability of the site for the incorporation of such features
- Topographic and climatic characteristics that could affect the performance of chemical or other windborne agents and other weapons
- The number of access and egress points, such as visitor entries, staff entries, and loading docks
- Internal vehicular (e.g., driveways, surface parking areas) and pedestrian circulation
- Location of high-risk areas within the school building that require access control and higher levels of security

This section reviews the most important of these characteristics from the perspective of security protection.

2.2.3.1 Location and Size

In most cases, the size of the site corresponds to its location in a metropolitan area or in a suburban or newly developed area. Urban schools sites are usually smaller and, because of the higher cost of land, schools have at least two to three stories. Sites in the suburban and newly developed areas on the periphery are much larger and usually have low lot-coverage ratios, which means that the school building can be placed farther away from streets and other public areas.

Site designers should work closely with the school building design team to integrate site and building design considerations. Initial concepts for the



In most cases, the size of the site corresponds to its location in a metropolitan area or in a suburban or newly developed area.

placement of the building(s) on the site provide the first opportunity to establish adequate standoff distances and delineate security perimeters.

Unless the site is a very high-risk site, school building placement based on construction and operational efficiencies may well take precedence over optimal security requirements for a rare or non-existent event.

2.2.3.2 Topography

The topography of the site is a very important security issue, because—depending on the placement of the school building on the site—it determines the opportunities for internal surveillance of site perimeters and screening of internal areas from external observation points. Building form, placement, and landscaping may help define the line of sight, and can facilitate effective control of potential hostile surveillance. Denying aggressors a line of sight, either from onsite or offsite, increases the security of the school buildings and their occupants.

Depending on the circumstances, topography can be either beneficial or detrimental with respect to surveillance. Elevated sites may enhance surveillance of the surrounding area from inside the facility, but may also allow observation of onsite areas by adversaries. Buildings placed immediately adjacent to higher surrounding terrain may be overly exposed to intrusive surveillance.

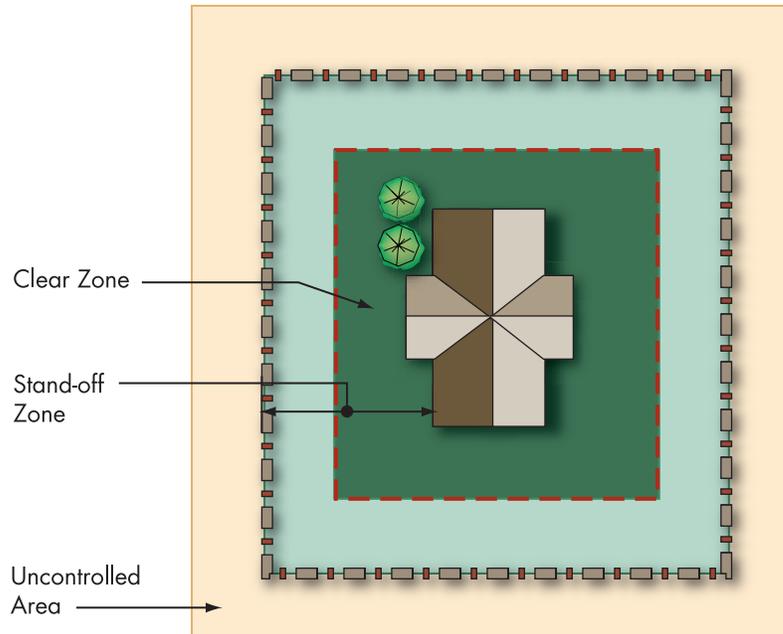
Schools in high-risk zones may require additional protection immediately adjacent to the structure in the form of a clear zone, free of all topographic obstructions or even landscaping that might provide hiding places (Figure 2-13). The clear zone facilitates monitoring of the immediate vicinity and visual detection of attackers or intruders.



Schools in high-risk zones may require additional protection immediately adjacent to the structure in the form of a clear zone, free of all topographic obstructions or even landscaping that might provide hiding places.

Figure 2-13:
Clear zone with unobstructed views

SOURCE: U.S. AIR FORCE,
INSTALLATION FORCE
PROTECTION GUIDE



2.2.3.3 Building Orientation

Orientation, or the physical positioning of a school building on site, can be a major factor for security. For the purpose of this primer, the term “orientation” refers to three distinct characteristics: a building’s spatial relationship to the site, its position relative to the sun and prevailing winds, and its vertical or horizontal aspect relative to the ground. A structure’s orientation relative to its surroundings defines its relationship to that area. In both aesthetic and functional terms, a building can “open up” to the area or turn its back; it can be inviting to those outside, or it can “hunker down” defensively.



Orientation, or the physical positioning of a school building on site, can be a major factor for security.

By optimizing the positioning of the school building relative to the sun, climate control and lighting requirements can be met while reducing power consumption. Similarly, the use of light shelves, skylights, clerestories, and atria can help meet illumination requirements while reducing energy usage. Light pipes supplying natural light through the roof or a hardened wall can reduce the size and number of windows needed, reducing energy usage and reducing the cost of hardening the building envelope.

Some of these energy conservation techniques have important security implications and must be examined carefully for their vulnerability to

blast loading and exposure to CBR agents. For example, although natural ventilation is an effective and time-tested technique for efficiently cooling buildings, the use of unfiltered outside air is a major vulnerability with respect to attacks with aerosolized CBR agents and accidental releases of hazardous materials. Similarly, operable windows may be more vulnerable to blast damage than the fixed ones.



School building organization, or plan configuration, directly affects the building's physical security and the ability of school authorities to monitor and enforce access control.

A structure's orientation in relation to the prevailing winds on site is significant characteristic with respect to the possibility of a CBR attack or hazardous material release. Wind may be beneficial in mitigating the effects of windborne hazards in that it reduces the concentration of agents in the air as distance from the source increases, spreading the plume laterally and upwind. The annual wind rose for the area is a good indicator of the probable distribution of wind speed and direction for a given period.

2.2.3.4 Building Configuration

School building organization, or plan configuration, directly affects the building's physical security and the ability of school authorities to monitor and enforce access control. Many suburban schools use the campus style of organization, with multiple single-story buildings spread around the school grounds. This type of organization is difficult to secure unless the perimeter is controlled and only a single access point to the school is maintained and monitored at all times. Nevertheless, the dispersed school buildings remain exposed to attacks from any direction.

A more compact organization of multiple school buildings, usually grouped around a central courtyard provides for easier surveillance and access control. By limiting the access to the inner courtyard and creating a secure enclosure, the school buildings' exposure to attack from the outside is significantly reduced. An even more compact organization involves a single building with a multi-story configuration or a single- or multi-story configuration with wings, such as U-, H-, or simple L-shaped plans. Though open, the courtyards formed by this type of school building are easier to monitor and control than the completely open grounds of a campus configuration. Figure 2-14 illustrates each type of school building configuration.

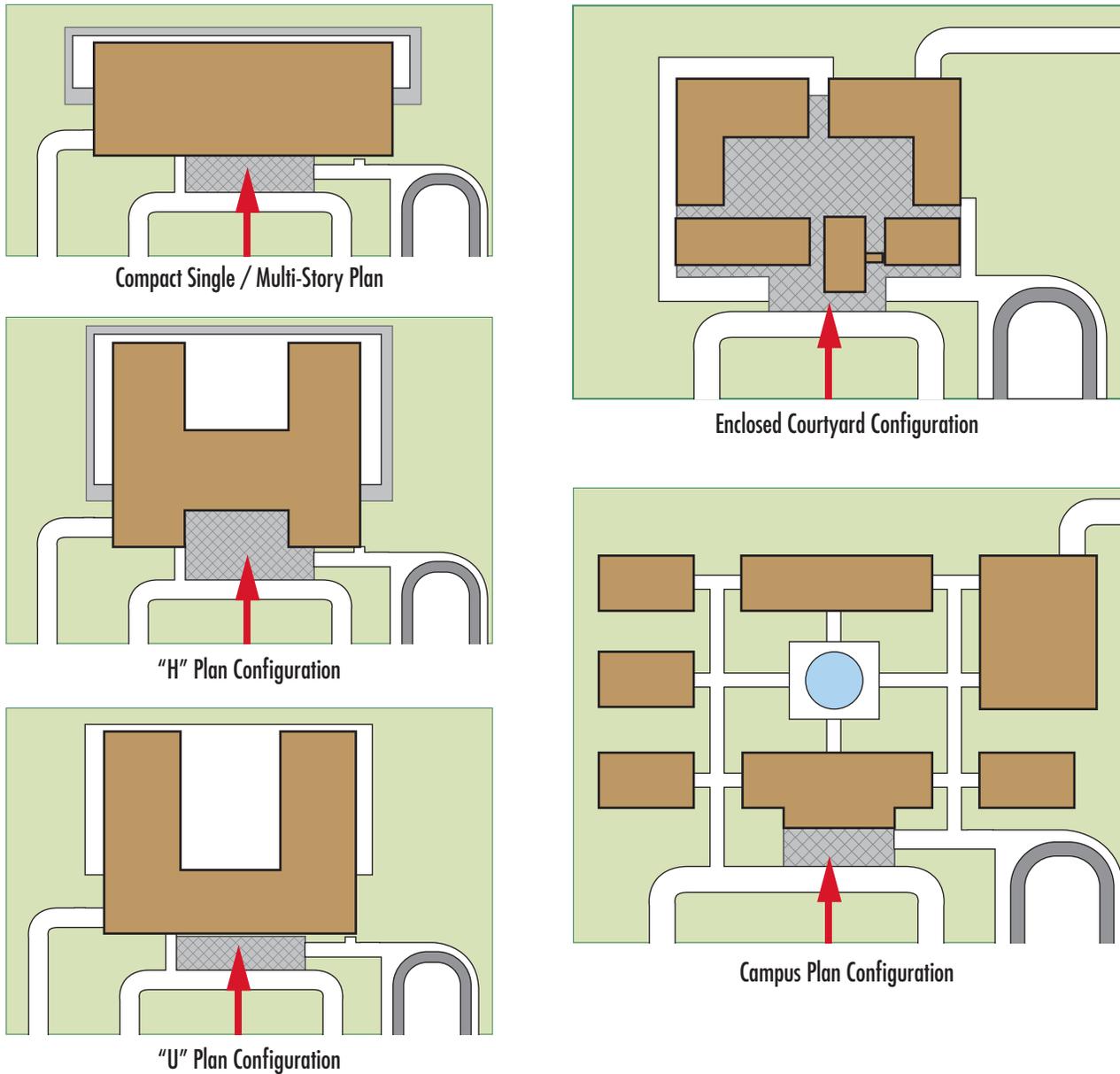


Figure 2-14: School building configurations

SOURCE: FLORIDA SAFE SCHOOLS DESIGN GUIDELINES, 2003

With respect to the attacks with explosive charge, the shape of the school building can contribute to the overall damage to the structure. For example, U-, H-, or L-shaped buildings tend to trap shock waves, which may exacerbate the effect of explosive blasts. For this reason, school buildings with re-entrant corners are much more vulnerable to blast damage (see Figure 2-15). In general, convex rather than concave shapes are preferred when designing the exterior of a school building.

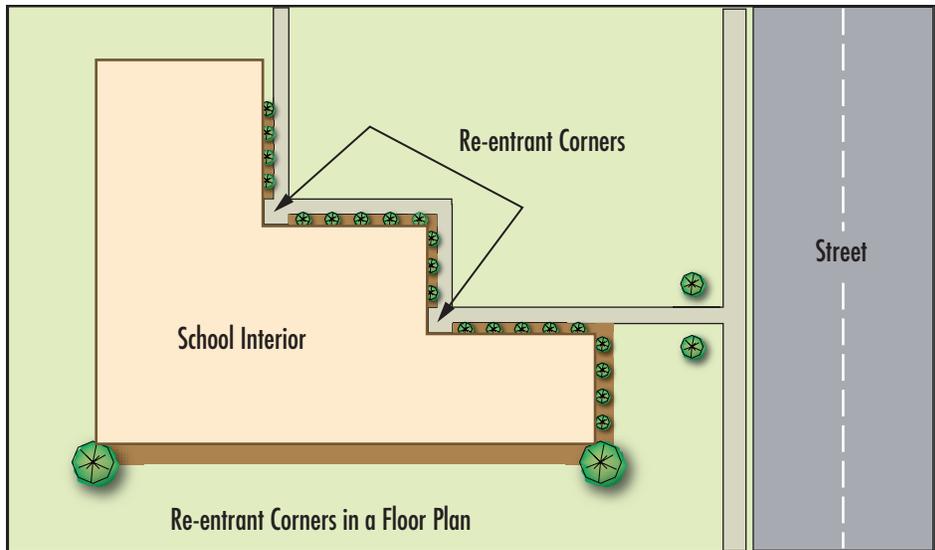


Figure 2-15:
Re-entrant corners in a floor plan

SOURCE: U.S. AIR FORCE, INSTALLATION FORCE PROTECTION GUIDE

Additionally, school buildings with the ground floor at grade are vulnerable to vehicles being driven into them. Similarly, building openings and glazed walls oriented toward publicly accessible areas increase the vulnerability of school occupants to attacks using explosives and various projectiles.

2.2.3.5 Vegetation

Vegetation onsite can open or block views for security purposes, as well as provide shade and enhance the appearance of the site (Figure 2-16). However, vegetation at the base of school buildings and structures may exacerbate certain vulnerabilities by obscuring views, providing hiding places for people and explosive devices, and facilitating surreptitious approach by potential attackers.

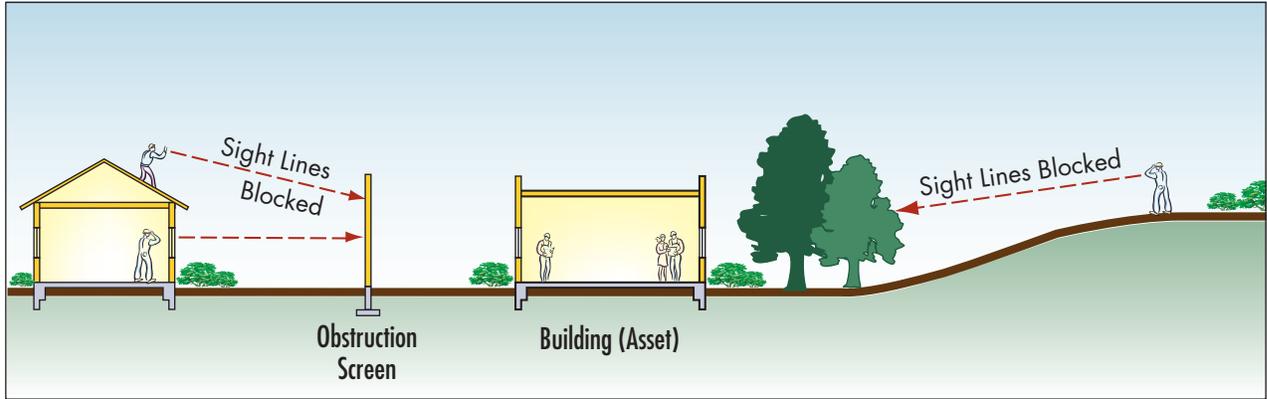


Figure 2-16: Trees and screens blocking sight lines into the site

SOURCE: U.S. AIR FORCE, INSTALLATION FORCE PROTECTION GUIDE

2.3 General Site Security Design Strategies

The fundamental objective of site planning is to place school buildings, parking areas, and other necessary structures in such a way as to provide a setting that is functionally effective as well as aesthetically pleasing. Increasing concerns for security add another dimension to the range of issues that must be considered.

The typical threats to a school, as discussed in Chapter 1, range from low to very low on the threat rating scale, and the risk is correspondingly low in a typical situation. However, the risk may increase with several rare but possible conditions, one of which is temporary and the other permanent, relating to the school location.

A temporary high-risk situation may arise if a series of attacks occur at nearby schools or similar facilities that require security to be enhanced for the period of concern. A typical example of this is the series of attacks by the so-called Beltway sniper that took place in the Washington, DC, metropolitan area during 3 weeks in October 2002. During that time, fear of the random shootings generated a great deal of public apprehension. A 13-year-old boy was shot as he arrived at the Benjamin Tasker Middle School in Bowie, MD, but he survived the attack. The attackers subsequently delivered a specific threat against children that was made public, and some schools cancelled all outdoor activities, such as field trips and outdoor athletics. Others changed after-school procedures for parents to pick up their children to minimize the time they spent in the open. Extra police officers were also assigned to the schools.

In some situations, heightened risk to schools may be long term or permanent and, therefore, require enhanced protective measures. One such situation is the possibility of collateral damage caused by an attack on an adjoining or nearby facility. A school may be located in proximity to high-risk facilities, such as major government buildings, or structures

with high symbolic value, such as bridges, iconic monuments, or national corporation headquarters buildings. The widespread collateral damage to buildings around the Murrah Federal Building in Oklahoma City (see Figure 2-17) is evidence of the magnitude of such risks.



The fundamental objective of site planning is to place school buildings, parking areas, and other necessary structures in such a way as to provide a setting that is functionally effective as well as aesthetically pleasing.

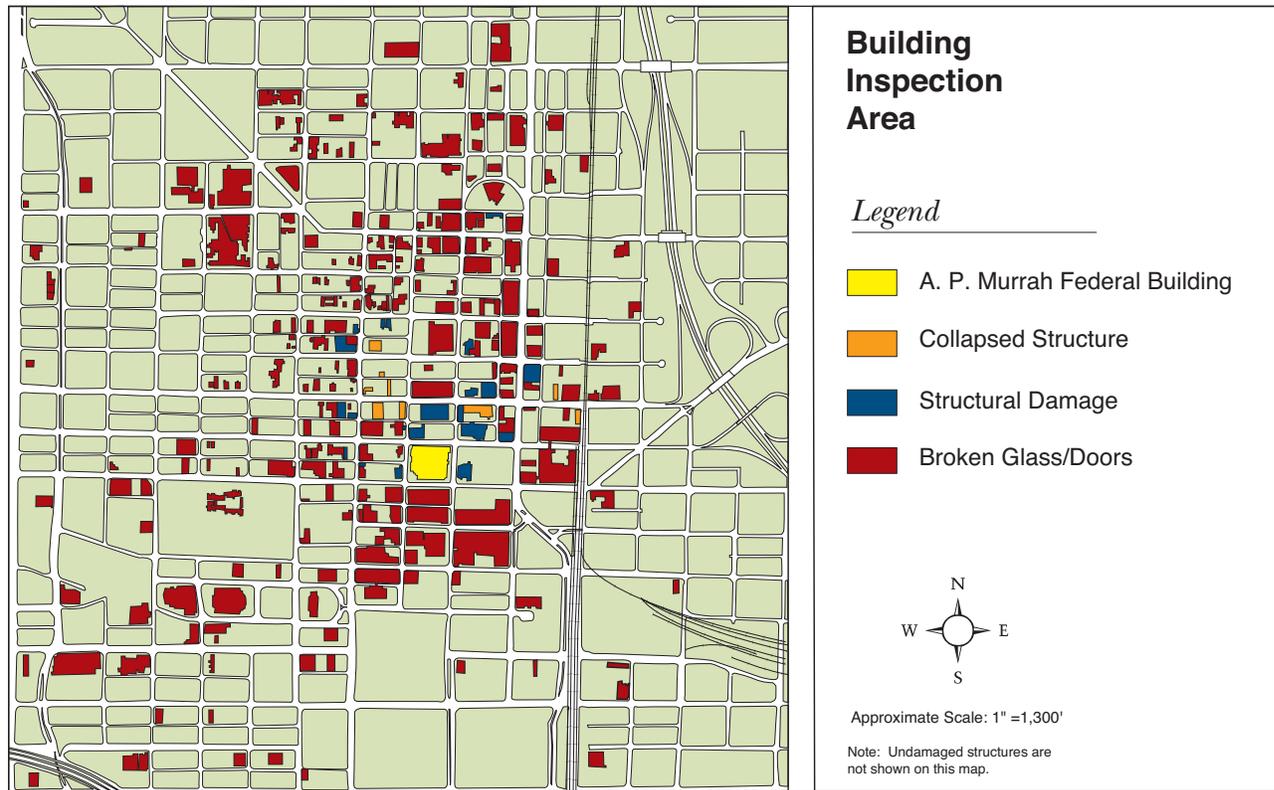


Figure 2-17: Collateral damage to buildings on sites adjacent to the Murrah Federal Building following the 1995 bombing

The design of protective measures for reducing site-related school vulnerabilities is based on a number of strategies that also represent the core principles of an effective security policy. They comprise the principles of a layered defense approach to security, standoff, access control, and a secure perimeter. Many of these principles are compatible with the Crime Prevention Through Environmental Design (CPTED) technique that has been used successfully to create a climate of safety in a community by designing a physical environment that positively influences human behavior. Although CPTED principles are not incorporated into the assessment process presented in this primer, CPTED is often entwined with protective measures against terrorist attacks.

CPTED is a methodology for crime prevention based on studies showing how physical design contributed to victimization by criminals. The methodology was originally applied to improve security in public housing, but now embraces wider aspects of criminality and terrorism. CPTED defines three basic strategies for security design: natural access control, natural surveillance and territorial reinforcement. For more details about CPTED, refer to www.cpted.net.

2.3.1 Crime Prevention through Environmental Design

CPTED concepts have been successfully applied in a wide variety of applications, including streets, parks, museums, government buildings, houses, and commercial complexes. The approach is particularly applicable to schools, where outdated facilities are common. Most schools in the United States were built 30 to 60 or more years ago. Security issues were almost nonexistent at the time, and technology was dramatically different. As a result, school building designs are not always compatible with today's more security-conscious environment.

According to CPTED principles, depending on purely conventional physical security measures (e.g., security guards and metal detectors) to correct objectionable student behavior or attacks from outside perpetrators may have its limitations. Although employing physical security measures will no doubt increase the level of physical security, in some cases physical security measures employed as standalone measures may lead to a more negative environment, thereby enhancing violence. In short, employing standalone physical security measures may fail to address the underlying behavioral patterns that adversely affect the school environment. CPTED analysis focuses on creating changes to the physical and social environment that will reinforce positive behavior.

CPTED builds on three strategies:

- Territoriality (using buildings, fences, pavement, sign, and landscaping to express ownership)
- Natural surveillance (placing physical features, activities, and people to maximize visibility)
- Access control (the judicious placement of entrances, exits, fencing, landscaping, and lighting)

A CPTED analysis of a school evaluates crime rates, office-referral data, and school cohesiveness and stability, as well as core design shortcomings of the physical environment (e.g., blind hallways, uncontrolled entries, abandoned areas that attract problem behavior). The application of CPTED principles starts with a threat and vulnerability analysis to determine the potential for attack and identify needs to be protected. Protecting a school from physical attack by criminals or terrorists, in many cases, only results in a change in the level and types of threats.



A CPTED analysis of a school evaluates crime rates, office-referral data, and school cohesiveness and stability, as well as core design shortcomings of the physical environment.

The CPTED process asks questions about territoriality, natural surveillance, and access control that can:

- Increase the effort to commit crime or terrorism
- Increase the risks associated with crime or terrorism
- Reduce the rewards associated with crime or terrorism
- Remove the excuses as to why people do not comply with the rules and behave inappropriately

The CPTED process provides direction to solve the challenges of crime and terrorism with organizational (people), mechanical (technology and hardware), and natural design (architecture and circulation flow) methods.

CPTED concepts can be integrated into expansion or reconstruction plans for existing buildings as well as new buildings. Applying CPTED concepts from the beginning usually has minimal impact on costs and results in a safer school. Each school, district, and community should institute measures appropriate for their own circumstances because no single solution will fit all schools.

Many CPTED crime prevention techniques for a school complement conventional terrorism and physical attack prevention measures. For example, as part of the CPTED strategy of improving territoriality, schools are encouraged to direct all visitors through one entrance that offers contact with a receptionist who can determine the purpose of the visit and the destination, and provide sign-in/sign-out and an ID tag prior to building access. These CPTED measures are similar to and complement physical security entry control point stations.

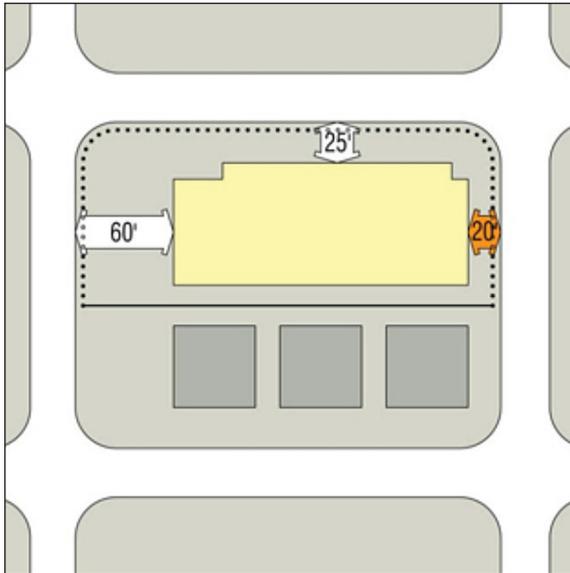
However, in some cases, CPTED techniques can conflict with basic physical security principles. The CPTED strategy of natural surveillance calls for locating student parking in areas that allow ease of monitoring. A design that locates student parking close to the principal's office also reduces vehicle standoff and could create a vulnerability of the school structure to a vehicle bomb. In cases for which CPTED techniques conflict with security principles, designers and school administrators should seek innovative solutions tailored to their unique situation.



The CPTED process provides direction to solve the challenges of crime and terrorism with organizational, mechanical, and natural design methods.

2.3.2 Standoff Distance

For the protection of assets against outside explosions, especially those associated with vehicle-borne explosive devices, the most cost-effective solution for mitigating blast effects is to ensure the explosion occurs as far away from the school building as possible.



This distance, from the building face to nearest point that an explosive device can approach from any side, assuming that all security measures are in place is referred to as the standoff distance or simply standoff (Figure 2-18).

For estimating purposes, the standoff distance is measured from the center of gravity of the charge located in the vehicle or other container to the face of the building under consideration.

2.3.2.1 Determining Standoff Distances

Determination of the minimum standoff is specific for each building or other asset and is based on the following:

Figure 2-18: Standoff distance

SOURCE: DAVID SHAFER

- Prediction of the explosive weight of the weapon (expected blast load provided by the threat assessment).
- Required level of protection, which may be specified in the case of a Federal or other government building, using the Interagency Security Committee (ISC) Security Design Criteria scale, Unified Facilities Criteria (UFC), or VA criteria; for a privately owned building, the determination of acceptable risk is made during the risk assessment process.
- Evaluation of the type of building construction, whether existing or proposed, including the building structure and the nature of the building envelope.

The U.S. Department of Defense (DOD) prescribes minimum standoff distances based on the required level of protection and expected blast load. Where minimum standoff distances are met, conventional construction techniques can be used with some modifications. In cases where the minimum standoff cannot be achieved, the building must be hardened to achieve the required level of protection. See UFC 4-010-02, *UFC DOD Minimum Standoff Distances for Buildings* (DOD 2003), and UFC 4-010-01, *UFC DOD Minimum Antiterrorism Standards for Buildings* (DOD 2007).

VA criteria limit unscreened vehicles from traveling or parking within 50 feet of their mission-critical facilities; screened vehicles may travel/park as close as 5 feet to the facility. For VA life-safety protected facilities, vehicles are permitted to travel or park up to 5 feet from the facility.

The ISC Security Design Criteria, which apply to new Federal Courthouses, Government Offices, and major modernization projects, also recommend standoff distances based on the level of protection for the facility, but do not prescribe a minimum distance. These recommended distances apply to vehicles that are parked on adjacent properties and for vehicles that are parked on the building site. The ISC Security Design Criteria recognize that different levels of protection may be permitted for the building structure and its façade so that they may be economically designed to appropriate levels of protection as discussed further in Chapter 4, Section 4.4, See *ISC Security Design Criteria for New Federal Office Buildings and Major Modernization Projects, Part 1 and Part II: Tables, Design Tactics and Additional Risk Guidelines* (ISC 2004), and *ISC Security Standards for Leased Spaces* (ISC 2004).

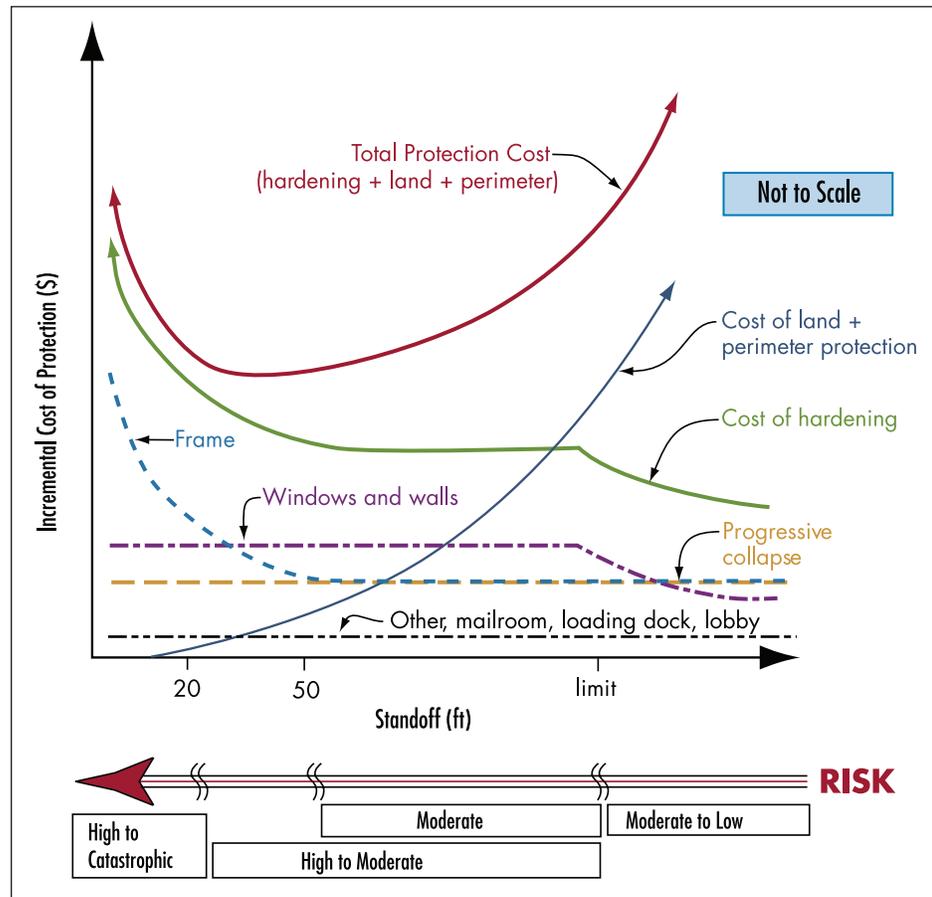
2.3.2.2 Constraints and Opportunities Provided by the Site

Because most open sites are able to provide considerable open space for standoff, conventional construction, with minor modification, may provide an acceptable level of protection against blast. However, a satisfactory standoff may be completely unachievable on a typical urban site, because the school building face may be only 10 to 20 feet from the curb, which is not an acceptable minimum distance from a potential blast. In such cases, alternative responses include protective measures, such as perimeter barriers, structural hardening, building envelope enhancement, operational procedures such as increased surveillance, or acceptance of some higher degree of risk.

At small standoff distances, even a few feet make a large difference in the blast loading. Increasing the standoff distance from 20 feet to 40 feet reduces the peak reflected pressure by a factor of four for a charge weight of 10 pounds and a factor of nearly seven for a charge weight of 1,000 pounds. The relationship between standoff distance and component cost is illustrated in Figure 2-19.

Figure 2-19:
Impact of standoff distance on
component costs

SOURCE: APPLIED RESEARCH
ASSOCIATES, INC.



For a more complete discussion of levels of protection, blast loading, standoff distance, and effects of blast see Chapter 4, Sections 4.3 and 4.4. See Section 2.3.2.3 for more detailed discussion of protective design for urban sites.

2.3.3 Layers of Defense

The basic approach to site security design promoted in this primer is the concept of layers of defense. These are multiple consecutive layers of protective measures deployed in concentric circles around a school. They start from the outer perimeter and move inward to the area of the

school building with the greatest need for protection. The layers are mutually independent and designed to reduce the effectiveness of an attack by attrition, i.e., each layer is designed to delay and disable the attack as much as possible. This cumulative protection strategy is also known as protection-in-depth, and has been one of the basic CPTED strategies for protecting assets behind



The basic approach to site security design promoted in this primer is the concept of layers of defense.

multiple barriers. Three main layers of defense emphasized in this publication are:

First or Outer Layer that consists of natural or manmade barriers usually at property line or sidewalk/curb line. Typically, the school perimeter is marked by no more than a fence, and is often completely open.

Second or Middle Layer usually extends from the perimeter of the site to the exterior face of a school building.

Third or Inner Layer starts at the building envelope and extends into the interior of the school building.



First Layer of Defense:

Consists of barriers usually at a property line or sidewalk/

curb line.

Second Layer of Defense: Extends from the perimeter of the site to the exterior face of a building.

Third Layer of Defense: Usually inside the building and separates unsecured from secured areas.

Most of the protective measures associated with the layers of defense are relevant for high- to medium-risk buildings; the precise measures are designed in response to the calculated blast threat and the desired protection level. These measures can be implemented in conjunction with CPTED procedures.

2.3.3.1 Layers of Defense for Single Building Open Sites

Most schools are constructed on an open site where the defended perimeter may or may not be on the property line. Typically, the perimeter barrier designates the standoff distance around the school building beyond which is the area that building owners and occupants do not control.

Figure 2-20 shows the whole site as an exclusive protected area; the perimeter barrier is located on the property line, and the onsite parking is within the second layer of defense. Crash-rated barriers are used where the site is vulnerable to invasive vehicles. The rear of the site is impassable to vehicles, so the barrier is limited to a fence to deter intruders.

An alternative solution is to place the barrier inside the property line, thus reducing its length. The onsite parking is outside the access-controlled area, and a minimum standoff distance is provided. Figure 2-21 illustrates an example of a site security design for an open site. Note the indirect approaches to the building and the variety of landscape details.

Figure 2-20:
Protective barrier located on the property line to provide required standoff and onsite parking within the protected area

SOURCE: FEMA 430

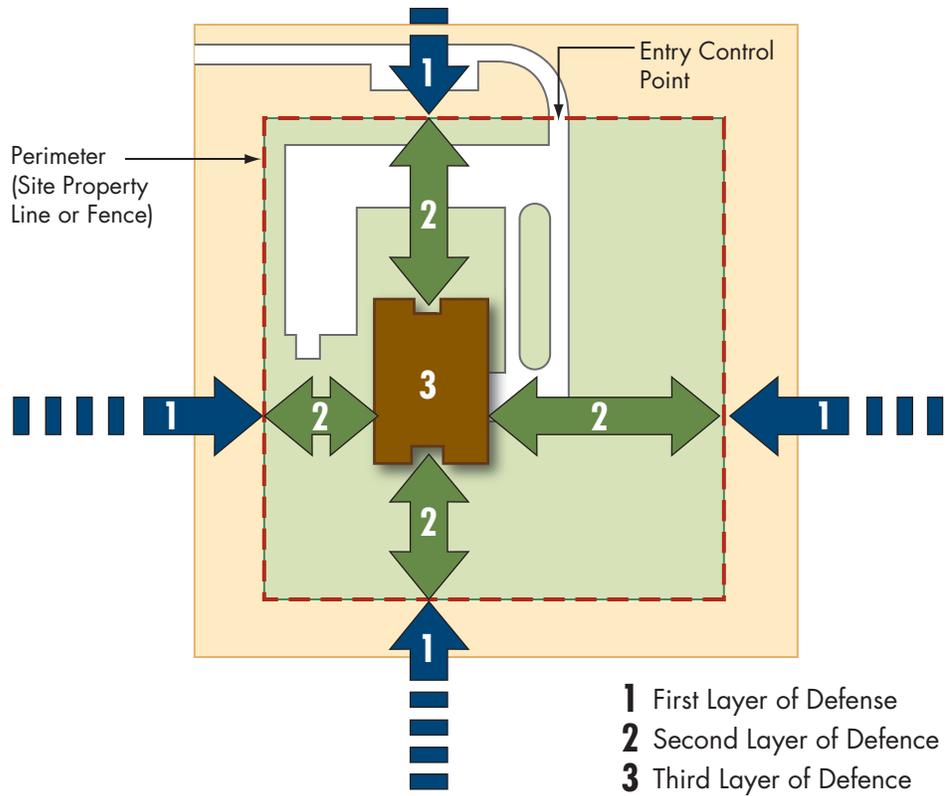
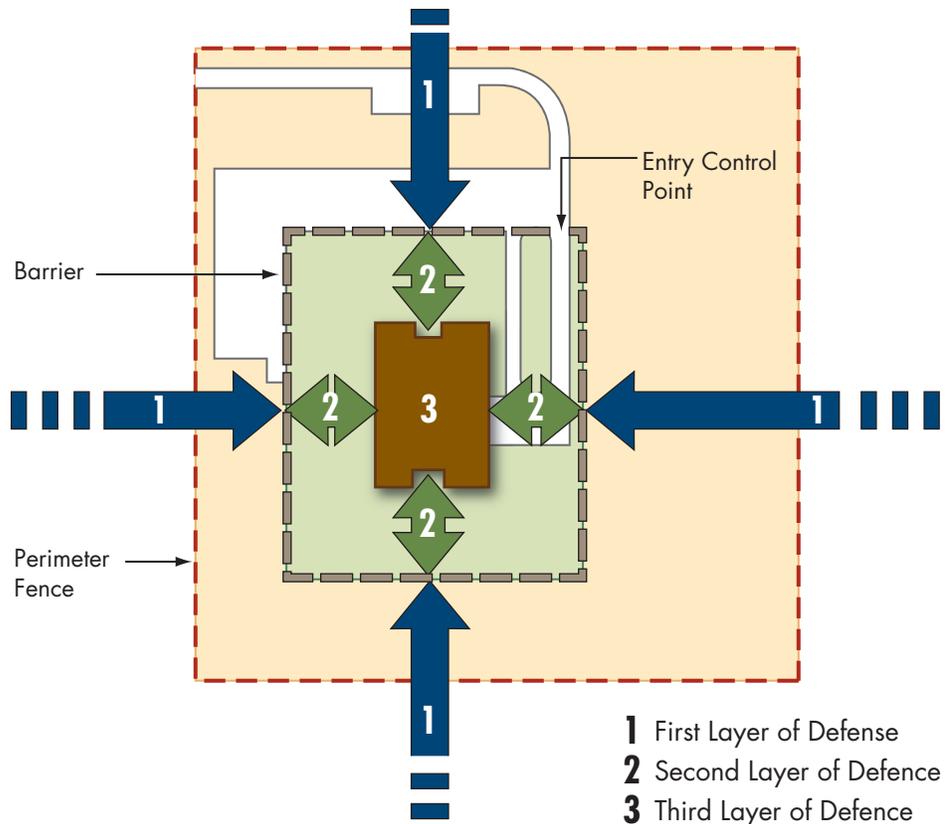


Figure 2-21:
Protective barrier located within the site providing minimum standoff

SOURCE: FEMA 430



2.3.3.2 Layers of Defense for Campus Sites

Layers of defense for a campus may take several forms, depending on the risk level for the campus as a whole as well as for individual buildings. The campus in Figure 2-22 shows a typical first line of defense at the transition between the first and second layers of defense; additionally, inside the fully protected perimeter, areas of the site also assume the role of first, second, and third lines of defense for one or more higher risk buildings.

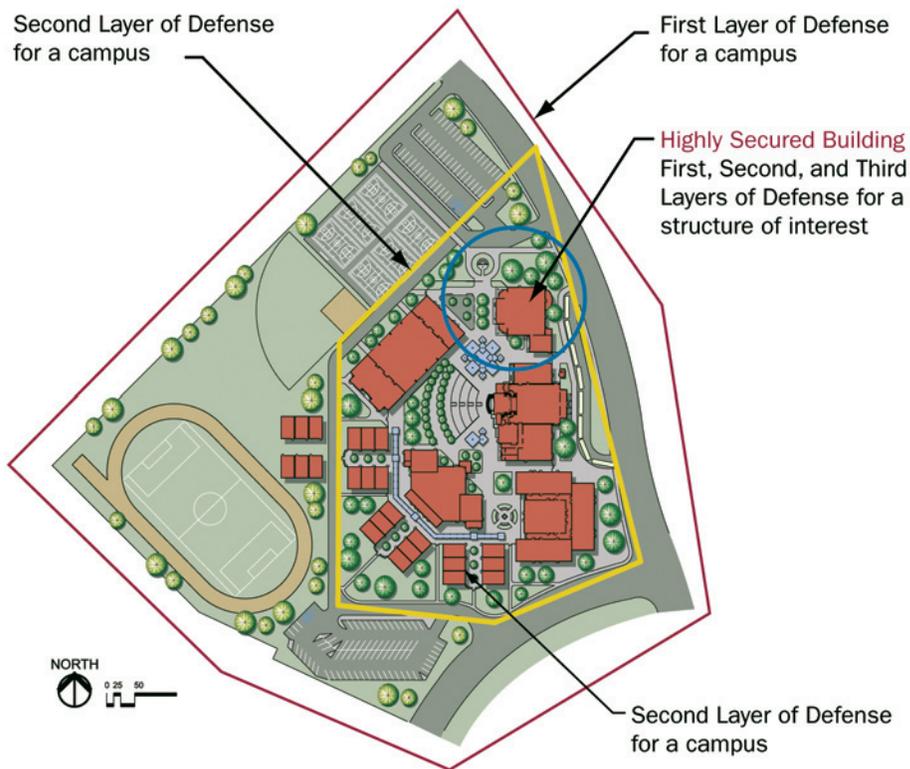


Figure 2-22:
Layers of defense for a campus site

SOURCE: WLC ARCHITECTS, INC.

In this example, the campus may have open access, but individual school buildings have varying protection, from minimal access control to the full three levels of defense around a high-risk building. In this latter case, the rest of the campus with first and second layers of defense becomes the first layer of defense for the high-risk building.

The campus may also have limited access control, as in a university that provides information and parking permits at entry points and a degree of security against common criminal activity. Specific high-risk buildings on a campus, such as laboratories, may have additional layers of defense.

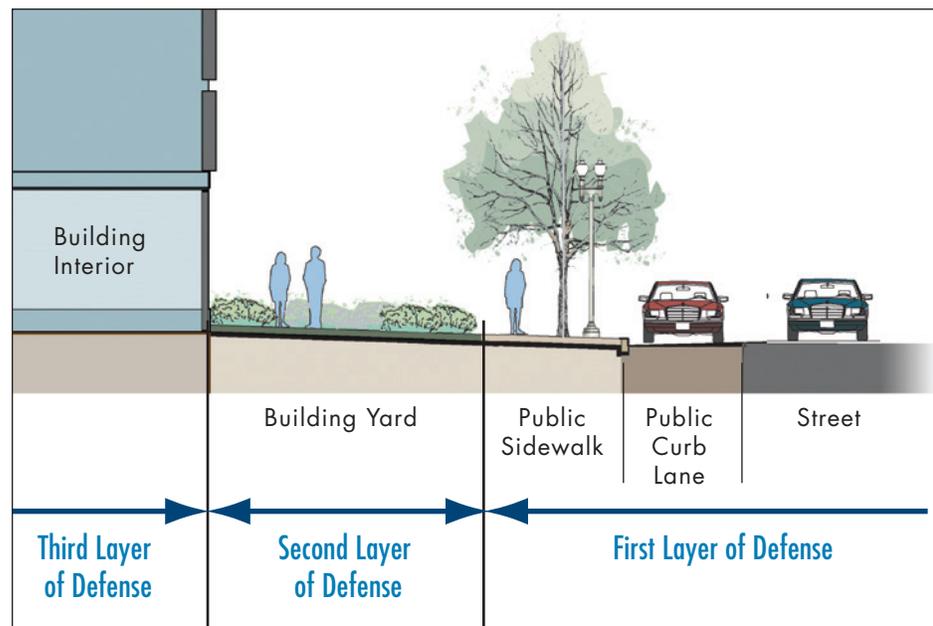
2.3.3.3 Layers of Defense for Urban Sites

Though less common, many schools are still found in busy urban neighborhoods on sites restricted in size, which has significant implications for site security design. In cases where the school façade is at the property line, the first layer of defense is usually outside the school property, typically on a public sidewalk. It may take on aspects of the second layer of defense if the school is granted permission to place vehicle barriers at the curb on municipal property. The third layer of defense then starts at the school building face, i.e., the property.

Most urban schools, however, have a yard between the building face and the sidewalk (Figure 2-23). The yard is within the property line and typically consists of a grassy or planted area adjacent to the building. In such cases, the curb lane and the sidewalk form the first layer of defense. The sidewalk serves as the common space for pedestrian movement, activity, and interaction. The building yard is the second layer of defense. In the yard, security components should complement the school building architecture and landscaping, because they will be easily visible from the sidewalk, and should be located near the outer edge of the yard. An engineered planter or plinth wall can provide a good security barrier for this layer. The third layer of defense is the face and interior of the building.

Figure 2-23:
Layers of defense with a yard

SOURCE: FEMA 430



2.3.4 Access Control

Access control is one of the key elements when determining effective placement of a school building. Designers should determine whether the building to be protected requires an exclusive or non-exclusive access zone (see Figure 2-24). An exclusive zone is defined as the area surrounding a single school building or building complex that is in the exclusive control of the owners or occupants: anyone entering an exclusive zone must have a legitimate reason. A nonexclusive zone may be either a public right-of-way, such as plazas, sidewalks, and streets surrounding a downtown school building, or an area related to several buildings, such as an industrial park with open access. The access-controlled zone may range from a complete physical perimeter barrier (full control) to relatively minimal anti-vehicle protection with full pedestrian access, or simple electronic monitoring of the perimeter.

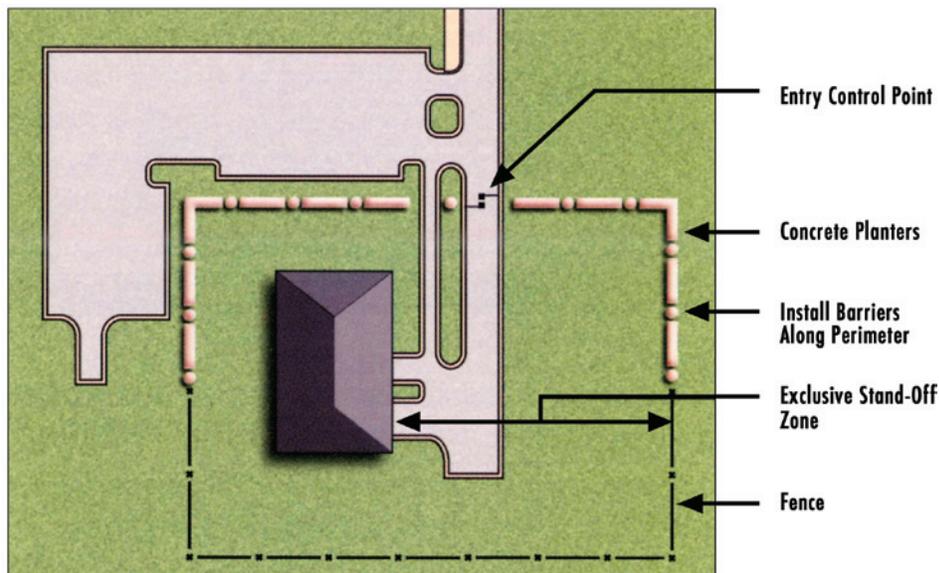


Figure 2-24: Exclusive zone within the site property

SOURCE: U.S. AIR FORCE
INSTALLATION FORCE
PROTECTION GUIDE

Some projects may require control of pedestrians and bicycles. In these cases, provision of a walkway and a turnstile for pedestrians (complying with the Americans with Disabilities Act [ADA] Accessibility Guidelines) should be considered.

2.3.4.1 Vehicle Approach Speed Control

The threat of vehicular attack can be reduced significantly by controlling vehicular speed and removing the opportunity for direct collision with the school building. If the vehicle is forced to slow down and impact a barrier at a shallow angle, the impact forces are reduced, and the barrier can be designed to lower performance requirements.

The speed of vehicles can be reduced by designing entry roads to sites and buildings that do not provide direct or straight-line access, making it impossible for a vehicle to gather speed as it approaches. Indirect approaches to a building, together with appropriate landscaping and earth forms, can also increase the attractiveness of the access road. Framing the sight of the school building by landscaping and other ways of controlling the views of the building can add to the aesthetic experience.

Figure 2-25 shows a portion of an analysis of threat vehicle approach speed used to determine the alignment and curvature of access roads to a large facility. The objective is to force the vehicle to impact the barrier at a reduced speed and at a shallow angle. This method also provides opportunities for enhancing the overall urban design of a site and its environs, as well as increasing pedestrian safety.

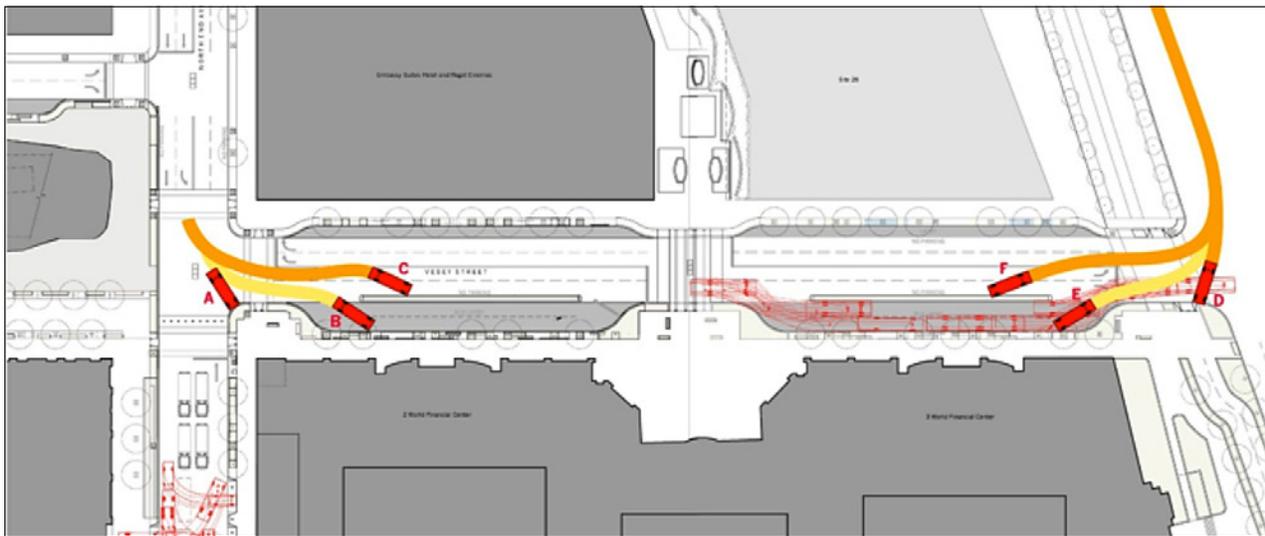


Figure 2-25: Portion of threat vehicle approach speed analysis

SOURCE: ROGERS MARVEL ARCHITECTS LLC

The following are some familiar devices and design methods of reducing vehicle speed:

- Traffic circles
- Curved roadways
- Chicanes (obstacle placement used to create a curved path on a straight roadway)
- Speed bumps and speed tables
- Raised crosswalks

- Pavement treatments
- Use of berms, high curbs, and trees to prevent vehicles from departing the roadway

Speed control of vehicles approaching gatehouses is also a concern. Some of the devices and design methods listed above can be used when approaching gates. In addition, bollards around the gatehouse can be used to narrow the approach. Truck entrances require wider lanes that can be handled by either active or removable bollards to limit the opening when trucks are not entering.

2.3.4.2 Entry Control and Vehicular Access

The objective of the access point is to prevent unauthorized access, while at the same time controlling the rate of entry for vehicles and pedestrians. An access point is a designated area for authorized school building users, such as employees, visitors, and service providers. Access points along the defended perimeter are commonly shared between the first and second layers of defense, providing observation of approach, controlled entry, and queuing areas. Structures such as control booths and equipment such as active barriers, communications, and video assessment and surveillance systems (VASS) (or closed-circuit television [CCTV])¹ are layered throughout the entry sequence to provide secured access points. Although the access itself is from a public roadway, these site features are within the site property line and form part of the first defense layer.



The objective of the access point is to prevent unauthorized access.

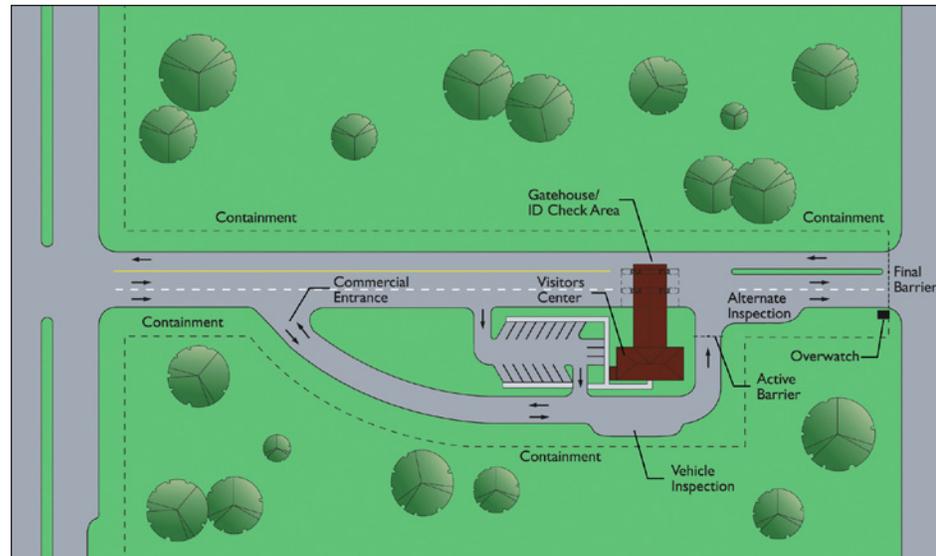
The location of access control points and inspection areas should be at sufficient standoff distance that detonation of a bomb on an uninspected vehicle does not impact the closest building and cause lethal damage. Figure 2-26 shows a typical layout of a high-security vehicle entry point and an access-controlled zone within a protected perimeter.

Whenever possible, commercial, service, and delivery vehicles should have a designated entry point to the site, preferably away from high-risk buildings. Active perimeter entrances should be designated so that security personnel can maintain full control without creating unnecessary delays. This can be accomplished by the provision of a sufficient number of entry points to accommodate the peak flow of pedestrians and vehicular traffic, as well as adequate lighting for rapid and efficient inspection.

¹ See Chapter 5. Because security video serves two distinct purposes, assessment and surveillance, the term used here is video assessment and surveillance system or VASS. Historically, the term for a security video system was CCTV, a closed analog video system.

Figure 2-26:
Typical entry control point
layout

SOURCE: U.S. AIR FORCE,
INSTALLATION ENTRY CONTROL
FACILITIES DESIGN GUIDE



The number of access points into a site should be minimized because they are a potential source of weakness in the controlled perimeter, and are costly to construct and operate. However, at least two access control points should be provided in case one is shut down by maintenance, bomb squad activity, or other causes.

2.3.5 Perimeter Security

A perimeter security system consists of two main elements: the perimeter barrier that prevents unauthorized vehicles and pedestrians from entering the site, and access control points at which vehicles and pedestrians can be screened and, if necessary, inspected before they pass through the barrier.

After 9/11, many cities experienced a proliferation of barriers, street closures, and other security measures around high-risk Federal and private buildings. In some cases, these measures have been considered successful from a security, architectural, urban planning, and cultural preservation standpoint. However, in many cases, the installation of security barriers has been acknowledged as detrimental to the function, quality, and utility of the public realm.

Restricting vehicle access can cause significant traffic congestion and can create unnecessary obstacles on streets and sidewalks that minimize the efficiency of pedestrian and vehicle circulation systems and hinder the access of first responders in emergencies.



A perimeter security system consists of two main elements: the perimeter barrier and access control points.

The following are suggested goals for perimeter security planning:

- Provide perimeter security in a manner that does not impede the city's commerce and vitality, excessively restrict or impede the use of sidewalks, limit pedestrian and vehicular mobility, or affect the health of existing trees.
- Provide security in the context of streetscape enhancement and public realm beautification, rather than as a separate or redundant system of components whose only purpose is security.
- Produce a coherent strategy for deploying specific families of streetscape and security elements in which priority is given to achieving aesthetic continuity along streets, rather than solutions selected solely by the needs of a particular building under the jurisdiction of one public agency.

Perimeter security protection is accomplished by design strategies that use a variety of methods to protect the site. The architecture and the landscaping of the site entry elements are the first part (and may be the only part) of the project that is visible to the general public. As such, they introduce the identity of the site, its architectural style and quality, and impart a sense of welcome or rebuff.

To achieve a welcoming atmosphere when incorporating security barrier systems, consider the following recommendations:

- Sidewalks should be open and accessible to pedestrians to the greatest extent possible, and security elements should not interfere with circulation, particularly in crowded locations.
- Barrier layout at sidewalks should be such that a constant clear path of 8 feet or 50 percent of the sidewalk, whichever is the greater, should be maintained.
- All necessary security elements should be installed to minimize obstruction of the clear path. They should be placed in an available amenity strip adjacent to most curbs, which is typically designated for street furniture and trees and not part of the existing clear path.
- Any security (or other) object placed at the curb should be at least 2 feet from the curb line to allow for door opening and to facilitate passenger vehicle pick-up and drop-off where permitted along the curb. Ideally, passenger drop-off points should be located in pullover or stopping points where the setback is greatest.
- Design and selection of barriers should be based directly on the threat assessed for the project, as well as available countermeasures and their ability to mitigate risk; excessive barriers should be avoided.

- Block after block of the same element, no matter how attractive, does not create good design. When a continuous line of bollards approaches 100 feet, it should be interspersed with other streetscape elements, such as hardened benches, planters, or trees.

Opportunities to add a palette of elements, such as varied bollard types, engineered sculptured forms, hardened street furniture, low walls, and judicious landscaping can all assist in creating a functional yet attractive barrier that will enhance the setting. Solutions that integrate a number of appropriate perimeter barriers into the overall site design will be more successful.

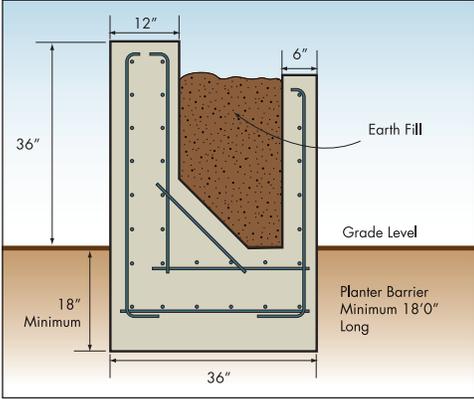
Barrier System Design Examples

Typical types of engineered (crash-rated) perimeter barriers are fixed bollards, engineered planters, fences, and retractable bollards. Each barrier is described further in Table 2-1.

Table 2-1: Engineered (Crash-Rated) Perimeter Barrier Types

Barrier Type	Descriptions, Installation, and Design Implications
<p>Fixed Bollards</p>	<p>A bollard is a vehicle barrier consisting of a cylinder usually made of steel and filled with concrete placed on end in a deep concrete footing in the ground to prevent vehicles from passing, but allowing the entrance of pedestrians and bicycles.</p> <p>Bollards can be specified with ornamental steel trim attached directly to the bollard or with selected cast sleeves of aluminum, iron, or bronze that slip over the crash tube.</p>  <p><i>Custom bollard covers</i> SOURCE: DELTA SCIENTIFIC INC.</p>  <p><i>A long line of bollards can appear as a wall.</i></p> <p>Installation:</p> <p>The need for bollards to penetrate several feet into the ground may cause problems with underground utilities whose location may not be known with certainty (see figure below). If underground utilities make the installation of conventional bollard foundations too difficult, bollards with a wide shallow base and a system of beams below the pavement to provide resistance against overturning (see figure below) are a possible solution.</p>

Barrier Type	Descriptions, Installation, and Design Implications
Fixed Bollards (cont.)	<div style="display: flex; justify-content: space-around;">   </div> <p data-bbox="420 741 721 768"><i>Installation of fixed bollard line (left)</i></p> <p data-bbox="420 779 656 804">SOURCE: SECUREUSA, INC.</p> <p data-bbox="907 741 1227 768"><i>Bollards on shallow beam system (right)</i></p> <p data-bbox="907 779 1276 804">SOURCE: RSA PROTECTIVE TECHNOLOGIES</p> <p data-bbox="420 827 602 854">Design Implications:</p> <p data-bbox="420 871 1370 957">Bollards are by their nature an intrusion into the streetscape. A bollard system must be very thoughtfully designed, limited in extent, and well integrated into the perimeter security design and the streetscape to minimize visual impacts.</p> <p data-bbox="420 978 1370 1123">To reduce the visual impact, bollard height should typically not be more than 30 inches. However, this height may be ineffective for some vehicular threats; for example, some States allow the maximum height of a bumper to be 31 inches (0.8 meter) above grade. Site-specific conditions, such as road surface grade and curb height, may help improve the effectiveness of a bollard for impact, while making the bollard appear less obtrusive.</p> <p data-bbox="420 1144 1370 1260">A bollard reduces the effective sidewalk width by the width of the curb to bollard (typically 24 inches [0.6 meter]) plus the width of the bollard. In high-pedestrian and narrow-sidewalk areas of a central Business district, the reduction in effective sidewalk width can be problematic.</p> <p data-bbox="420 1281 984 1308">Other bollard system guidelines include the following:</p> <ul data-bbox="420 1329 1370 1850" style="list-style-type: none"> • Bollard spacing should be between 36 and 48 inches (0.9 and 1.2 meters), depending on the kind of traffic expected and the needs of pedestrians and the handicapped. • Where a long line of bollards is unavoidable, the bollards can be interspersed with trees and oversize bollards that can act as seats. In a few years, the trees will dominate the streetscape, and the barriers will be unobtrusive. • Bollards should be kept clear of ADA access ramps and the corner quadrants at streets. • Bollards should be arranged in a linear fashion in which the center of the bollards is parallel to the centerline of existing streets. • Bollards may be custom designed for an individual project to harmonize with the materials and form of the building; but to provide adequate protection, they must be tested by an independent laboratory. • Closely spaced bollards can also make the navigation to curb cuts particularly challenging for wheelchairs. • In no case should bollards exceed a height of 38 inches (1 meter), inclusive of any decorative sleeve.

Barrier Type	Descriptions, Installation, and Design Implications
<p>Fixed Bollards (cont.)</p>	 <p><i>A long line of bollards with trees interspersed (left). Custom bollards used in conjunction with a sloping wall barrier (right).</i></p>  <p><i>Corner installation of custom concrete bollards that match the building architecture.</i></p>
<p>Engineered Planters</p>	<p>Well-designed planters can form an effective vehicle barrier. Planters located on the surface rely on friction to stop or delay a vehicle and will be pushed aside by any heavy or fast-moving vehicles; displaced planters may become dangerous projectiles.</p> <p>Engineered planters need considerable reinforcing and below-grade depth to be effective and become fixed elements in the landscape design. The planter shown provides a Department of State (DOS) K12 rating.</p>  <p><i>Typical engineering detail of reinforced planter with DOS K12 performance</i></p>  <p><i>Planter with concealed crash-rated bollards SOURCE: WAUSAU TILE</i></p>

Barrier Type	Descriptions, Installation, and Design Implications
<p>Engineered Planters (cont.)</p>	<p>Installation:</p> <p>Some guidelines for planter system installation include the following:</p> <ul style="list-style-type: none"> • Rectangular planters should be no more than 2 feet (0.6 meter) wide and 6 feet (1.8 meters) long, and circular planters should be no more than 3 feet (0.9 meter) in diameter. • A maximum distance of 4 feet (1.2 meters), depending on the kind of traffic anticipated, should be maintained between planters and other permanent streetscape elements. • Planters should not be used in high pedestrian traffic areas. • Planters should be oriented in a direction parallel to the curb or primary flow of pedestrian traffic. In no case should a planter or line of planters be placed perpendicular to the curb. • Landscaping within planters should be kept below 2.5 feet (0.8 meter) in height, except when special use requirements call for increased foliage. Depending on the threat, consideration should be given to ensuring that a 6-inch-high (15-centimeter-high) package could not be concealed in the foliage. <p>Design Implications:</p> <p>Planters can have a major impact on pedestrian movement, reducing the effective sidewalk width. However, well-designed and placed planters can have multiple functions and be civic amenities.</p>  <p><i>These planters are formed by the top of retaining walls (left). Alternating bollards and planted retaining walls as a barrier (right).</i></p>
<p>Fences</p>	<p>Fences are a traditional choice for security barriers, primarily intended to discourage or delay intruders or serve as a barrier against standoff weapons (e.g., rocket-propelled grenades) or hand-thrown weapons (e.g., grenades, fire-bombs). Familiar fence types include:</p> <ul style="list-style-type: none"> • Chain-link • Monumental fences (metal) • Anti-climb (CPTED) fence • Wire (barbed, barbed tape or concertina, triple-standard concertina, tangle-foot)

Barrier Type	Descriptions, Installation, and Design Implications
<p>Fences (cont.)</p>	<p>These fence types are primarily intended to delay intrusion. They provide very little protection against vehicles, but they can act as a psychological deterrent when an aggressor is deciding which building to attack. Fencing can also incorporate various types of sensing devices that relay warning of an intruder to security personnel.</p> <p>Fences can be constructed as engineered anti-ram systems. An effective solution is to use cable restraints to stop the vehicle: these can be placed at bumper height within the fence and hidden in plantings.</p> <div data-bbox="500 548 1073 995" data-label="Image"> </div> <div data-bbox="1105 548 1349 632" data-label="Caption"> <p>Crash-rated fence SOURCE: AMERISTAR FENCE PRODUCTS INC</p> </div> <div data-bbox="500 1024 760 1083" data-label="Caption"> <p>Layout of cable fencing, used in conjunction with planting</p> </div> <div data-bbox="500 1100 760 1192" data-label="Text"> <p>SOURCE: DOD HANDBOOK: SELECTION AND APPLICATION OF VEHICLE BARRIERS, MIL-HDBK-1013/14, 1999</p> </div> <div data-bbox="789 942 1463 1451" data-label="Diagram"> </div> <p>Installation:</p> <p>Cable system fences allow considerable deflection and partial penetration of the site before resistance occurs. The amount of deflection is based upon the distance between the concrete "dead men," typically about 200 feet. As a result, the installation requirements for fences and gates that incorporate a cable system differ slightly from other types of walls and fences.</p> <p>Design Implications:</p> <p>Fences for the protection of property have a long history and have also often been elements of great beauty. Modern fences are governed more by function and cost, but variations of historic fence design have been used as barriers for important historic building. The appearance of less attractive fencing can be improved by plantings.</p>

Barrier Type	Descriptions, Installation, and Design Implications
Retractable Bollards	<p>A retractable bollard system consists of one or more rising bollards operating independently or in groups of two or more units. The retractable bollard is a below-ground assembly consisting of a foundation structure and a heavy cylindrical bollard that can be raised or lowered by a buried hydraulic or pneumatic power unit, controlled remotely by a range of access control devices.</p> <p>Typical retractable bollards are 12 to 13 inches (30 to 33 centimeters) in diameter, up to 35 inches (0.9 meter) high, and are usually mounted 3 feet (0.9 meter) apart, depending on typical traffic.</p> <p>Retractable bollards are used in high-traffic entry and exit lanes where vehicle screening is necessary, at site entrances, and at entries such as parking garages and building services. Unlike rising or rotating wedge systems, the entry is freely accessible to pedestrians when the bollards are raised.</p> <p>Normal bollard operating time is field adjustable and ranges from 3.0 to 10.0 seconds. Emergency operating systems can raise bollards to the guard position from fully down in 1.5 seconds.</p> <p>Installation:</p> <p>Retractable bollards are expensive because they need broad and deep excavation for the bollards and operating mechanisms. Also, as with all active barriers, they require regular maintenance to ensure continued operation.</p> <p>Design Implications:</p> <p>Retractable bollards are relatively unobtrusive barriers that need only to be raised when screening is necessary. A retractable bollard system is generally accompanied by fixed bollards at the sides, and a secure control booth is necessary for security personnel.</p>  <p><i>Typical retractable bollard systems at a service entry; note fixed bollards at sides</i></p>

- In areas subject to chemical spills, a school sited in a depression or low area may be trapped by heavy vapors and natural decontamination by prevailing winds may be inhibited.
- Outdoor containers in which explosives can be hidden (such as garbage cans, mailboxes, and recycling or newspaper bins) should be kept at least 30 feet from the school building and be designed to restrict the size of objects placed inside them, or to expose their contents (for example by using steel mesh instead of solid walls).
- In areas considered susceptible to explosive attack, the standoff distance between buildings and the nearest parking or roadway should be at least 75 feet with more distance for unreinforced masonry or wooden walls. If this standoff is not achievable, the creation of additional standoff protection by barriers and parking restriction should be considered.

2.4 Parking

2.4.1 Parking in Open Sites

Parking on open sites is typically accommodated by surface parking lots. On-street parking lanes may occur on any site but are particularly characteristic of urban areas.

All parking in an open site should be located outside the standoff zone for high-risk buildings. Access control may be necessary at the entry to parking in non-exclusive zones for regulation and fee collection. If the site has a perimeter barrier, authorization to enter the site and any necessary inspection can take place at entry control points; parking structures should not need additional control.



All parking in an open site should be located outside the standoff zone for high-risk buildings.

Warning signs that are easy to understand should be installed along the physical barriers and at each entry. An important design goal is the development of an efficient layout of the parking spaces and provision of an internal circulation that has clear paths for pedestrians and vehicles. Parking restrictions can help to keep potential threats away from a school building. Operational

measures may also be necessary to inspect or screen vehicles entering parking areas.

The following considerations may help designers to implement sound parking measures for schools that may be at high risk:

- Only permit parking by inspected vehicles within the standoff zones and avoid or limit drop-off zones.
- Provide appropriate setback (standoff) from parking to the protected school building. Structural hardening may be required if the setback is insufficient. In new designs, adjust the location of the building on the site to provide adequate setback from adjacent properties, if possible.
- If possible, locate unexpected visitor or general public parking near, but not on, the site itself, or outside the standoff zone.
- Locate vehicle parking away from high-risk school buildings to minimize collateral blast effects from potential vehicle bombs.
- Locate general parking in areas that present the fewest security risks to personnel.
- If possible, design the parking lot with one-way circulation to facilitate monitoring for potential aggressors.
- Locate parking within the view of occupied school buildings. Use carefully chosen plantings around parking structures and parking lots to permit observation of pedestrians while at the same time reducing the visual impact of automobiles. Topography, existing conditions, or aesthetic objectives may make this difficult or undesirable to achieve, and CCTV surveillance cameras may substituted.
- Do not permit uninspected vehicles to park within the exclusive zone or in the second layer of defense.
- Restrict parking between individual school buildings, especially when the buildings are relatively close together, because the proximity increases reflected blast pressures.
- Provide emergency communication systems (e.g., intercom, telephones, etc.) in establishing parking areas at readily identified, well-lighted, CCTV-monitored locations to permit direct contact with security personnel.
- Provide parking lots with CCTV cameras connected to the security system and adequate lighting capable of displaying and videotaping lot activity.

2.4.1 Public Street Parking

In urban areas, public street parking is often located within a desired standoff zone. Evaluation of the viability of this option must consider the role of the street within the local infrastructure, whether the municipality must be reimbursed for loss of metered parking income, and whether an additional lane provides significant improvement of the standoff distance.

If street parking lanes are unacceptable because of the high risk, access to the vulnerable streets and parking may have to be prohibited to create an adequate standoff zone. This approach has been adopted in the New York City Financial District. Street closure has serious implications for everyday function and accessibility, and should only be undertaken if no other solution, such as building hardening, is feasible.

Considerations for public street parking include the following:

- Request appropriate permits to restrict parking in curb lanes in densely populated areas to company-owned vehicles or key employee vehicles.
- Provide appropriate setback from parking on adjacent properties, if possible. Structural hardening may be required if the setback is insufficient. In new designs, adjust the location of the school building on the site to provide adequate setback from adjacent properties, if possible.
- Pick-up and drop-off areas should have appropriate barriers at the edge of the curb to enforce standoff distances for unscreened vehicles and to address mobility and convenience for pedestrians. Barriers should be placed at a distance from the curb to allow clearance for vehicle doors to open (24 inches minimum), the provision of adequate lighting and shelter so pedestrians can wait safely for their rides, and appropriate design for handicapped access. Circulation planning should ensure that effective access is available for first responders and other emergency vehicles.