ATLAS SAFETY & SECURITY DESIGN, INC.

DESIGNING AGAINST TERROR: SITE SECURITY PLANNING AND DESIGN CRITERIA

As published in **Architectural Graphics Standards**: 1999 Revision

By Randall Atlas Ph.D., AIA
Atlas Safety & Security Design, Inc.
Miami, Florida

1. Statement of the Problem

The first contact a person has with a particular architectural project is accessing the site to gain entry to a property or building. With the increasing threats to persons and property, from acts of terrorism, workplace violence, and street crime, the first and most important line of defense is securing the site perimeter and the careful placement of the building/s on the given site.

Architects design buildings that serve a particular function for the users and clients of a building, and hopefully do it in a pleasing aesthetic manner. But also important in fulfilling this task, this design should protect that user, ensuring their safety and security in the environment. The main guardian of health and safety for building designs are building codes, but these only address architectural features, such as egress design, fire safety, structural integrity, stair proportions, and railing design, while ignoring the considerations of crime or terrorism. As safety is a prime consideration of building codes, security of the site and building users should be considered a high priority.

2. Assessment Process

Achieving the correct level of protection against site-based threats may be very expensive and is highly dependent on the nature of the protected assets and the threat against which they require protection. Determining what is required is a matter of managing the perceived risks. If the designer is to assist in providing protection in the design of the site, an assessment of the security requirements must be accomplished, preferably before the design begins, but certainly no later than the beginning of the programming phase. This assessment is the responsibility of the owner; however, it is incumbent on the designer to assure that the nature of the security requirements is determined before the design begins. Failing to obtain a definitive answer will certainly result in design changes, delays, and cost increases to the owner and the architect if the owner “discovers” their security needs later in the design process.

The site assessment will answer the following four questions. What are the assets (persons , places, information, property) that require security protection? What are the criminal or other threats (street crime, workplace violence, terrorism, sabotage) against which the assets must be protected? What are the vulnerabilities of the assets to the threats (for example, if workplace violence is a threat, can uncontrolled persons enter private workspace unchallenged)? What are the countermeasures (for example, does the design channel visitors through controlled site access portals) required to mitigate the threat?

The result of the assessment will be a set of recommended countermeasures that may be priced and presented to the owner in a priority order so selections may be made of those recommendations that are prudent and cost effective. In the case of the government standards, the assessment results in the assignment of a defined Level of Protection (LOP) with specified countermeasures. When the LOP is defined, the specified countermeasures are priced and again the owner may select appropriate measures depending on a prudent level of protection and the cost effectiveness of the measure.

3. Security Layering: the Onion Philosophy

The first layer is the outside skin of the onion which translates to the site perimeter of the property. The building skin of the architecture is the next layer. Sensitive areas within a building are deeper layers requiring protection, and finally special persons information or property may require point protection or the center of the onion.

The site perimeter is the first, not last, line of defense. The State Department seeks setbacks of at least 100 feet for new buildings, and even at that distance it is difficult to obtain in most urban settings. While most perimeter fences and walls are designed to discourage intruders, they are of little use against a determined person or bomb vehicle. Designs are now available for vehicle-stopping capabilities. However, the bomb of the future may be delivered by a moped or pedestrian, thus rendering truck bombs unnecessary.

4. The GSA Security Standards

The bombing of the Murrah Federal Office Building in Oklahoma City gave birth to a federal effort to develop security standards that would apply to all federal facilities and an Interagency Security Committee has recommended their adoption as a government wide standard. During the testing of the standards, a number of state governments also reviewed the standards and applied them to several new construction projects. Consult local and state authorities for their specific applications.

The process of risk assessment and security design is especially relevant in architecture of schools, hospitals, airports, office buildings, multi-family apartment buildings, etc. Recently, buildings have been targeted for bombing by terrorists because of their “architectural vulnerability”. This vulnerability will be addressed by methods described in this section.

The GSA Security Standards encourages a Defensible Space/Crime Prevention Through Environmental Design (CPTED) approach to clearly defining and screening the flow of persons and vehicles through layering from public to private spaces. Edges and boundaries of the properties should clearly define the desired circulation patterns and movements. The screening and funneling of persons through screening techniques is the effort to screen legitimate users for the building from illegitimate users who might look for opportunities to commit crime, workplace violence, or acts of terrorism.

The result of approximately one year of work by the GSA panel is a set of Criteria covering four levels of protection for every aspect of security addressed by the U.S. Marshals report. The U.S. Marshall’s report made a large number of recommendations for both operational and equipment improvements. The GSA Security Standards addresses the functional requirements and desired application of security glazing, bomb resistant design and construction, landscaping and planting designs, site lighting, and natural and mechanical surveillance opportunities (good sight lines, no blind spots, window placement, proper applications of CCTV). These recommendations were further subdivided according to whether they should be implemented for various levels of security (e.g. a level one facility might not require an entry control system while a level four facility would require electronic controls with CCTV assessment). Those requirements of the report which affect facility design and engineering are presented here in four general categories of corrective action used in the report.

The following should be addressed by the architect and engineering team for renovations or new construction on any federal building and is recommended for state and local buildings:

1) PERIMETER & EXTERIOR SECURITY

Parking area and parking controls
CCTV Monitoring
Lighting to include emergency back up
Physical Barriers

2) ENTRY SECURITY

Intrusion detection system
Upgrade to current life safety standards
Screen mail, persons, packages
Entry control with CCTV and electric door strikes
High security locks

3) INTERIOR SECURITY

Employee ID, Visitor control
Control access to utilities
Provide emergency power to critical systems
Evaluate location of Day Care Centers

4) SECURITY PLANNING

Evaluate locations of Tenant Agencies as concerns security needs and risk
Install Mylar film on exterior windows
Review/establish blast standards for current projects and new construction
Develop a design standard for blast resistance and street set-back for new construction

The criteria take a balanced approach to security, considering cost effectiveness, acknowledging acceptance of some risk, and recognizing that Federal buildings should be not bunker or fortress-like, but open, accessible, attractive, and representative of the democratic spirit of the country. Prudent, rather than excessive, security measures are appropriate in facilities owned by and serving the public.

5. Application of GSA Security Standards to all building types

Whatever the building or its use, security and crime prevention should be a design criteria, similar to fire safety, accessibility, and structural integrity. Any piece of architecture should establish a hierarchy of space that go from open access by the public, to semi-public, to semi private, to private spaces. Any areas or spaces that are unassigned to a specific purpose or capable guardian should be avoided as it becomes “no man’s land” and not claimed, protected, or defended by any individual or group. Traffic patterns of pedestrians and vehicles into sites and buildings should be carefully thought out and controlled for the desired goal. The design of any building should maximize the potential for natural observation by the legitimate building users.

Key defensive architectural site design considerations for bomb resistance:

Establish a secured perimeter around the building that is as far from the building as is feasible. Setbacks of 100 feet are desired.

Design artistically pleasing concrete barriers as flower planters or works of art and position them near curbing at a distance from the building, with less than four feet of spacing between them to block vehicular passage.

Build new buildings in a simple geometric rectangular layout to minimize the “defraction effect” when blast waves bounce off U-shaped or L-shaped buildings causing additional damage.

Drastically reduce or totally eliminate ornamentation on buildings which can easily break away causing further damage to building occupants or pedestrians at street level. All external cladding should be made of light-weight materials that will minimize damage when they become flying objects following an explosion (or hurricane!).

Eliminate potential hiding places near the facility.

Provide unobstructed view around the facility.

Site or place the facility within view of other occupied facilities.

Locate assets stored on site, but outside of the facility within view of occupied rooms of the facility.

Minimize the signage or indication of assets on the property.

Provide a 100 foot minimum facility separation from the facility boundary if possible.

Eliminate lines of approach perpendicular to the building.

Minimize the number of vehicle access points.

Eliminate or strictly control parking beneath facilities.

Locate parking as far from the building as practical (yet address ADA spaces and proximity) and place parking within view of occupied rooms or facilities.

Illuminate building exterior or exterior sites where assets are located.

Secure access to power/heat plants, gas mains, water supplies, electrical and phone service.

6. Application of security standards to other building types:

The process can apply to all forms of architecture:

Institutional architecture: police stations, courthouses, jails and prisons, post offices, schools, hospitals, airports .

Commercial architecture: Office buildings, shopping centers, retail stores, restaurants, entertainment facilities.

Residential architecture: Single family homes, townhouses, low-mid-high rise multi-family residential facilities, planned urban developments, hotels, rental apartments, public housing.

7. Security and Design: Crime Prevention Through Environmental Design (CPTED)

Crimes are committed because they are easy to commit. A person sees an easy opportunity and so they do it, regardless of the legality or consequences. Casual criminals are eliminated by increasing the effort needed to commit a crime. Target hardening is one method of increasing the effort using the increased use of fencing, landscaping and plantings, and curbs. Another technique of CPTED is natural access control which includes installing symbolic and real barriers, designing paths walkways and roads so that unwanted and unauthorized users are prevented from entering vulnerable areas. Barriers may include limiting entrance to specific individuals, places or times, security vestibules, parking lot barriers, entry phones, visitor check-in booths, guard stations, vehicle control systems, and bio-metric screening for access control.

Site considerations include:

Control access to the facility by pedestrian and vehicular traffic.

The number of entrances to the interior of a building should be minimized , with the function of the remaining entrances clearly identified. Entrances should be secured when not in use.

Control parking lot access by means of gates and passes.

Install barriers on vulnerable openings such as ground floor windows, exterior fire stairs, roof openings, and skylights.Fence off problem areas to prevent unauthorized access and funnel movement along desired paths.

Control access for servicing and deliveries.

Vacant lots, apartments, offices, and spaces should be used or given to legitimate users to protect against vandalism and damage.

Exterior walls should be painted with graffiti resistant epoxy and/or landscaped with creeping vines to prevent the wall from acting as a mural for graffiti taggers.

8. CONCLUSION

The GOAL for architects and design professionals: Minimizing fortress design and target hardening, except where required AFTER thorough analysis and study. The design professional must address the issue of how architectural design features and approaches can enhance security without intruding objectionable aesthetics and functionality of the building.

Site Security Design elements can include:

Bollards/planters
Curbs
Vehicle barriers
Security lighting
Signage and groundrules
Gates

Site Security Systems Elements:

Consider space for placement of hardware and servicing.
Plan for generous wiring.
Plan for backup power.
Plan for intrusion detection device.s
Plan for site intrusion detection.
Plan for boundary penetration sensors.
Plan for motion detection systems.
Plan for access control systems.
Plan for contraband and weapons detection.
Plan for explosive detectors.
Plan for credential readers and positive personnel identification systems.
Plan for security control and information display systems.
Conduct the need assessment and include it as part of the architectural programming.
Determine the level of criticality and threats to the building assets.
Change how people use the building for legitimate authorized uses.
Use security technology last, once the circulation patterns are clear and the architecture of form reflects the function of facility.
Use the national standards as a starting point to establishing a standard of care in order to improve efficiency , safety and security and to reduce premises liability from negligent security design and practices.

9. Where to get more information

GSA Security Standards.
ASIS (American Society of Industrial Security): Web: www.asis.com
CPTED: Web: www.cpted-security.com
www.spartacc.com
www.ncjrs.org
BOMBCAD - Everett Brown Co. 950 N Meridian ST. Indianapolis, In. 46204, 317-237 7043
SECURITY LIGHTING - Illumination Engineering Society.

Written by Dr. Randall I. Atlas, AIA, CPP of Atlas Safety & Security Design Inc., Miami , Florida; Anthony DiGreggario, Applied Research Associates, Washington DC.; and the input of the Security Architecture and Engineering Committee of the American Society of Industrial Security.