Security Planning and Design Guidelines

The University of Texas System

Office of Facilities Planning and Construction

F Foreword

The *Security Planning and Design Guidelines* is a tool to help the component institutions of The University of Texas System assess potential threats and plan security provisions for their capital improvement projects.

These guidelines are generic in nature and are intended to be used for both academic and health affairs projects, including projects of a primarily engineering nature.

We recommend that the component institutions refer to the guidelines during the development of their CIP submissions, during preparation of the Facilities Program for projects, and during the design of projects.

T Table of Contents & Revision Log

Chapter		Page	Revision Date
Introductory Materials:			
Purpose of this Document		i.1	
Introduction		ii.1	
Getting Started		iii.1	5/15/03
***Guidelines*:**			
1	Security Assessment	1.1	
	Asset Definition	1.1	
	Threat Profile	1.3	
	Vulnerability Analysis	1.5	
2	Security Planning	2.1	
	Security Objectives	2.1	
	Physical Design Elements	2.5	
	Site Development	2.5	
	Site Lighting	2.7	
	Landscaping	2.9	
	Utilities	2.9	
	Parking	2.10	
	Exterior Building Configuration	2.12	
	Interior Building Configuration	2.14	
	Structural Considerations	2.17	
	MEP Considerations	2.20	5/15/03
	Security Systems Elements	2.31	
	Access Control System	2.34	
	Intrusion Detection and Alarm Monitoring (IDAMS)	2.36	

Emergency Assistance
Communications 2.37
Closed Circuit Television
Surveillance System..... 2.38
Operational Elements..... 2.40

a **Appendices:**

Acknowledgments.....a.1.1
References a.2.1
Resources for Additional Information.....a.3.1 5/15/03

Notes Regarding the May 15, 2003 Revision:

Revised and new items are identified by underlined text and "5/15/03"in the right margin.

i Purpose of this Document

The events of September 11, 2001 and other related threats since that date have raised public awareness regarding security issues, as well as expectations that those entrusted with planning and designing public facilities are making adequate provisions to mitigate security risks.

This document is designed as a tool to assist component institutions to identify and minimize potential security threats during the planning and design of facilities.

The guidelines are not intended to prescribe mandatory security measures that must be incorporated in every facility. Rather, they are intended to provide a checklist of issues to consider and options for addressing security concerns.

The guidelines are generic in nature to allow for their flexible application to all project types at any institution.

We anticipate that security provisions for additional projects can be integrated with campus planning and operations.

At this time, each of the component institutions in the U. T. System are in the process of reassessing potential threats to their campuses, evaluating their vulnerability to these threats, and formulating a comprehensive response to them. Just as each institution is unique, their updated campus security plans will be formulated to address the unique needs of their institutions.

These guidelines focus on the planning and design of physical and electronic control measures for new projects. While security operations is also a significant aspect of a comprehensive campus security plan, this document does not make specific recommendations regarding security operations or practices. However, it should be emphasized that inadequate physical and electronic security provisions for a facility will result in a greater reliance on operational measures, such as police patrols, which historically result in greater long-term costs. Therefore, we recommend that campus security operations representatives participate in the evaluation and selection of physical and electronic control measures that will best meet their needs while minimally impacting their operating budgets.

This document was assembled using published resource information from public and private entities identified in *Appendix a2. – References* and is current as of the date

of this issuance. We recommend that project teams refer to *Appendix a3. – Resources for Additional Information* to gather the latest information regarding the topics identified.

ii Introduction

Although security provisions are a part of most capital improvement projects, the measures adopted are often developed on a project-by-project basis, without adequate consideration of how the project fits within the overall security plan for the campus. These guidelines recommend that a systematic and comprehensive process be used to assess security threats. As a result of the process, specific threat mitigation measures will be considered and perhaps incorporated into the project design. This process begins when the institution first identifies a project concept, prior to its inclusion in the U. T. System Capital Improvement Plan (CIP). The process continues through the programming, design, procurement, and construction phases of the project.

The best time to influence the security design of a facility is when the project concept is first identified. Consideration of the proposed function(s) of the facility will guide site decisions that optimize security needs. Institution representatives responsible for preparation of the biannual CIP submission will review the guidelines when preparing their CIP worksheets to ensure that they consider security issues when determining a project's preliminary scope and cost.

The specific scope of security requirements will be described in more detail and quantified when the Facilities Program is prepared. When preparing the program, we recommend that the institution select an outside consultant with specialized expertise in comprehensive security analysis to be a member of the programming team, which will also include campus user groups, local campus Police Departments, and Environmental Health and Safety Department representatives. The security analysis and recommendations for the project will be recorded in the program and reflected in the detailed project scope description and preliminary project cost.

The project team will continue to refer to the guidelines during the project design process as security needs identified during programming are translated into design solutions. It is important to refer to security recommendations developed in the Facilities Program while preparing and evaluating design options. Design options that most effectively support the security goals should be given precedence over those that do not. Also, it is important to consider physical and electronic security provisions as critical components of projects, not discretionary ones that are subject to cutting when project budgets become tight. Inadequate budgeting for the physical security design, or reductions in the quantity and quality of electronic control measures, may

result in the need for increased staffing for security operations that will be more expensive over the lifetime of the facility.

Certain types of projects must meet security requirements set by regulatory agencies in order to receive the desired certification and/or funding from that agency. Each institution should review the applicable regulatory agency's security requirements to determine the more stringent requirements.

High-risk projects may require restricted access to project documentation, such as architectural drawings and project specifications. The project team should evaluate the need for restricted access to sensitive project-related data.

iii Getting Started

This document is divided into two major chapters, the **Security Assessment** section and the **Security Planning** section. The **Security Assessment** section assists the project team in determining a project's security requirements. The **Security Planning** section provides guidelines for the planning of security measures that will be incorporated into the project to mitigate the risks identified during the security assessment.

As previously stated, we recommend that this document be used during:

- CIP Preparation
- Programming
- Design

CIP PREPARATION

During CIP preparation, the component institution will refer to the **Security Assessment** section of the *Guidelines* for help in determining the overall suitability of a building use or type to a proposed site on the campus and in identifying potential problems before programming and/or design stages begin.

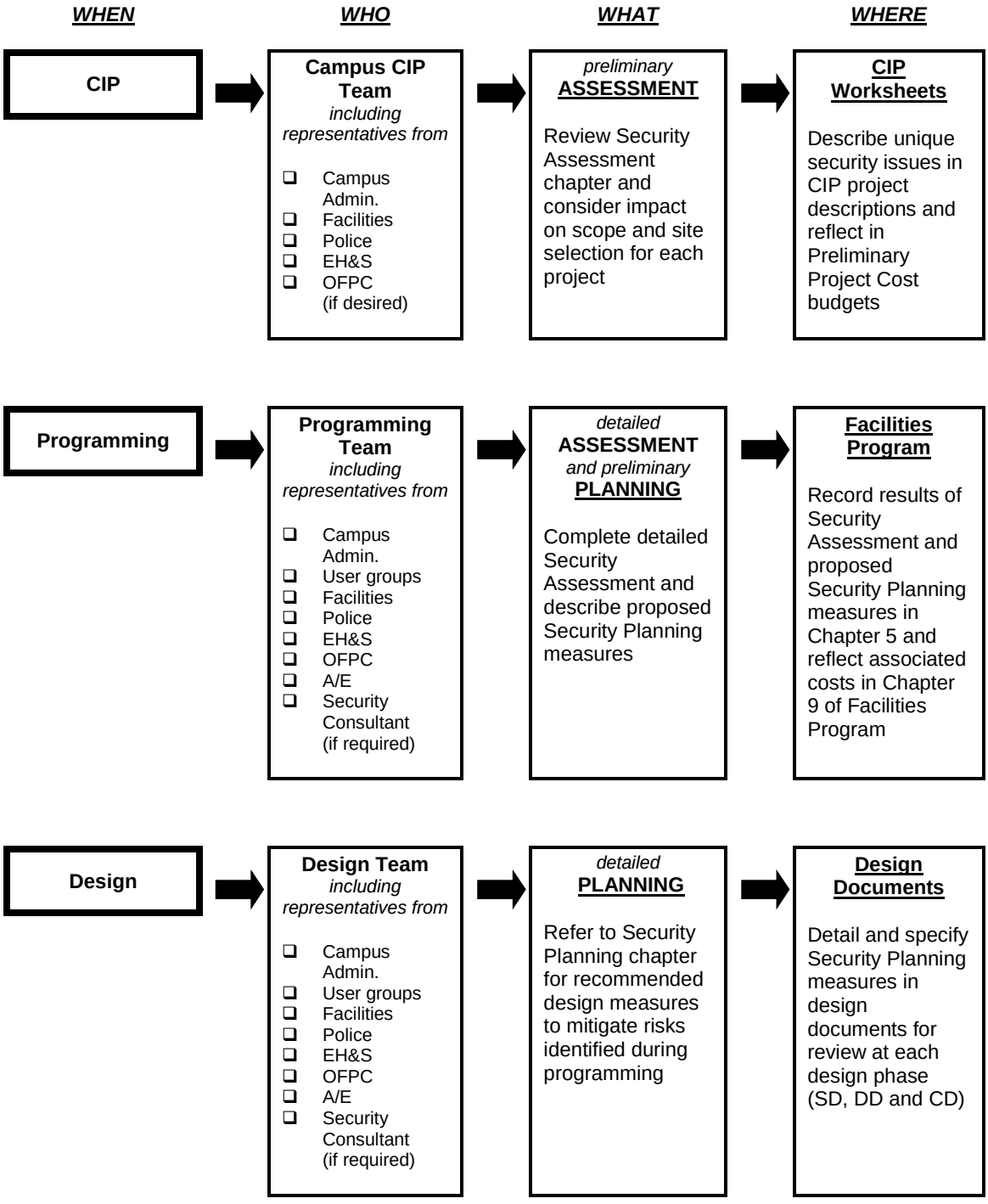
The guidelines in this document also apply to significant lease properties. Consider the nature of usage of the leased facility and the duration of the lease period.

PROGRAMMING

If not done during CIP preparation, we recommend that the project team complete the **Security Assessment** section of the *Guidelines* during the programming phase. The information gathered during the assessment process will be recorded in the Facilities Program for the project under *Chapter 5 – Supporting Requirements*. The project team will then review the recommendations in the **Security Planning** section of the *Guidelines* to preliminarily identify the security measures that will be necessary to mitigate the risks identified during assessment. The project team will document the proposed security measures in the program. The team will quantify and estimate the costs of the security measures reflected in the program under *Chapter 9 – Preliminary Project Cost.*

DESIGN

We recommend that the project team refer to the **Security Planning** section of the *Guidelines* during the design phase of the project to assist in determining the security design measures necessary to address the risks identified in the security assessment completed during programming.


WHEN
WHO
WHAT
WHERE
CIP
Campus CIP Team
including representatives from
Campus Admin.
Facilities
Police
EH&S
OFPC (if desired)
preliminary
ASSESSMENT
Review Security Assessment chapter and consider impact on scope and site selection for each project
CIP Worksheets
Describe unique security issues in CIP project descriptions and reflect in Preliminary Project Cost budgets
Programming
Programming Team
including representatives from
Campus Admin.
User groups
Facilities
Police
EH&S
OFPC
A/E
Security Consultant (if required)
detailed
ASSESSMENT
and preliminary
PLANNING
Complete detailed Security Assessment and describe proposed Security Planning measures
Facilities Program
Record results of Security Assessment and proposed Security Planning measures in Chapter 5 and reflect associated costs in Chapter 9 of Facilities Program
Design
Design Team
including representatives from
Campus Admin.
User groups
Facilities
Police
EH&S
OFPC
A/E
Security Consultant (if required)
detailed
PLANNING
Refer to Security Planning chapter for recommended design measures to mitigate risks identified during programming
Design Documents
Detail and specify Security Planning measures in design documents for review at each design phase (SD, DD and CD)

PROCESS DOCUMENTATION 5/15/03

It is important to format the information documented for use in the planning and design of the facility in a way that readily facilitates its use by the project team in tracking and confirming that the each of the threats to and vulnerabilities of the assets identified in the Security Assessment process have specific mitigation measures identified for them in the Security Planning process. For this purpose, it is recommended that the results of the assessment and planning be summarized in a tabular format, similar to the below example.

← Security Assessment →	← Security Planning →
Asset (what are you protecting?)	Threat/Vulnerability (from what?)	Mitigation Measure (how?)
(continue for each Asset)		

This format will provide a checklist for the project team to use in confirming that the security planning and design process effectively mitigates the security risks of the facility.

1 Security Assessment

The security assessment is the first stage in determining the security needs for a project. Each project team will conduct a risk assessment to determine the level of security to apply to the project. The project team can conduct this assessment alone or with the assistance of an outside consultant; however, we strongly recommend the participation of an outside consultant.

Prior to making decisions regarding the application of security measures for a project, the project team must understand the security dynamics surrounding the project. A variety of factors including project type, project location, local crime statistics—both from campus and surrounding community perspectives—and user group security requirements drives the dynamics. Determining these dynamics will guide the team in identifying potential security issues, a topic which will be addressed in the **Security Planning** section of the *Guidelines*. The first step in the assessment phase, however, is Asset definition.

ASSET DEFINITION

The purpose of asset definition is to establish priorities for protection against identified threats. Because it is

impossible to protect every asset against every possible threat, a process to determine which assets will be protected based on how critical and valuable each is to the organization must be used.

❑ Identify Assets

A project's assets are those things that you wish to protect. Assets can be people (staff, students, guests), real property (the building and parking facilities), and/or other property (computers, databases, electronic files, lab equipment, etc.).

❑ Prioritize Assets

After identifying the project assets, prioritize the assets to determine the correct level of security necessary to protect them. Categorize assets as follows:

- Vital – Loss could be catastrophic to the operation of the project or campus.
- Important – Loss would be disruptive but not catastrophic to the operation of the project or campus.
- Secondary – Loss would be unpleasant but relatively insignificant to the operation of the project or campus.

Once the assets for the project have been defined, develop a threat profile to determine what level of security is required to adequately safeguard the assets.

THREAT PROFILE

The threat profile will include an assessment of a project's risks and the ranking of those risks or threats. We developed the recommendations in this guide to address the security needs of a wide variety of building types constructed by The University of Texas System. Apply these recommendations to your project in direct proportion to the type of facility proposed and the risk assessment for the project.

❑ Develop past local incident profile

Review with the local campus police department any past incidents that have occurred in the last four years that might affect the project's intended use. Document any unique, significant, or extraordinary incident that may have occurred in the last 10 years if the team feels it may be relevant to the project.

❑ Review past local crime statistics

Review past incidents in the surrounding neighborhood with the local police department to identify any local criminal history that might affect the project.

❑ Threat Identification and Analysis

After interviewing the appropriate local personnel to determine the past history of incidents in and around the proposed site, catalogue each incident. Index all past incidents under the following categories:

1. Conventional criminal acts against persons such as homicide, robbery, rape, and aggravated assault.

2. Conventional criminal acts against property such as burglary, larceny, and motor vehicle theft.

3. Criminal acts involving chemical agents.

4. Criminal acts involving biological agents.

5. Criminal acts involving radiological agents.

6. Accidents that involve agents such as chemical, biological, or radiological.

7. Natural disasters such as tornados, floods, fires, hurricanes, and/or earthquakes. While these events cannot be controlled or avoided, occurrence of such events may direct the project team to make provisions to mitigate the effect they can have on the security of a project. Examples of such mitigating provisions would include locating critical power equipment above the flood plain in a building or locating critical security equipment in an area of high survivability.

When the threat profile is complete, merge the assets definition and the threat profile to perform the vulnerability analysis.

VULNERABILITY ANALYSIS

The primary objective of the vulnerability analysis is to determine how to mitigate the potential threats against an identified asset. First, define the method of compromise to which the asset is subject; then, develop a plan to mitigate the compromising action.

The next section addresses the potential methods of compromise, or how the assets might be attacked, stolen, or destroyed. In reviewing the following items, the desired result is determining how to reduce the risk of the design elements being used to encourage or assist in the event.

❑ Identify building usage

Building usage and/or type may dictate the required level of security. Review those elements associated with a project usage to ascertain the need for additional security measures. Give special consideration to high-risk usage buildings such as nuclear reactors, animal holding facilities, Biosafety Level 3 or 4 labs, etc.

For example, a laboratory building containing research animals might require additional protection for the research animals and the research staff against animal rights groups. A nuclear engineering lab might require enhanced security to meet federal DOE requirements.

❑ Determine adjacent facilities

Review all adjacent buildings to determine the ownership and control. Determine use of adjacent buildings and how their use might affect the proposed project. Review for potential of collateral damage from and to adjacent facilities.

When warranted by a risk assessment, consider acquiring adjacent sites or negotiating for control of rights-of-way. Where possible, separate new projects as far as possible from adjacent properties not owned by the U. T. System.

❑ Analyze proposed site

Define site security requirements, including perimeter buffer zones, before a site is selected or the construction funding request is finalized. These requirements may preclude the selection or purchase of a site because it lacks the necessary features, especially setback, or because it needs costly countermeasures such as blast hardening.

❑ Review the topography

Review the topography of the proposed site to determine whether the site has any natural vulnerabilities that need to be corrected or offers any potential to naturally support the required security.

❑ Determine appropriateness of fencing or walls

Determine appropriateness of perimeter fencing or walls to secure site for vehicular control or for building perimeter protection.

❑ Review existing site utilities

Analyze all underground and overhead utilities near the proposed project site to determine whether any precautions are required to safeguard the project from accidental or intentional damage from use of an existing utility as an instrument in perpetrating an incident.

SECURITY ASSESSMENT CHAPTER REVIEW

When completed, the security assessment will provide valuable data about the specific security threats facing a project. At this point you know the facility location and what impact it might have on the building or its occupants, whether the surrounding buildings and/or community pose a danger to the project, and what the criminal history in the area has been for the past two to four years. Carry this information forward to the security planning phase and use it to determine the security measures necessary to mitigate the defined threats.

2 Security Planning

SECURITY OBJECTIVES

The security planning process for any project begins once the security assessment process is complete and the potential threats have been defined. Security planning is a multifaceted endeavor involving all aspects of the project design. Prior to looking at the design-related issues, the planning process objectives should be reviewed.

The major objectives of security planning are to:

- DEFINE – Security planning should define the space, creating definable and identifiable boundaries to inform both guests and users of public and restricted areas.

- DETER – Security planning should provide for both physical and psychological deterrents to criminal activity on the property.

- DETECT – Security planning should provide a system for early warning of potential intruders that leaves sufficient time to observe, prevent, and/or respond to the incident.

SECURITY MUST BE AN INTEGRAL PART OF THE BUILDING AND SITE PLANNING, STARTING AT THE EARLIEST PHASE AND CONTINUING THROUGHOUT THE PROCESS.

- MONITOR – Security planning should provide the capability to observe and monitor intruders and/or security incidents. This monitoring and observation should be accomplished through the use of varied levels and patterns of detection/deterrent devices and closed circuit television (CCTV) surveillance.

- INTERVENE – Security planning should incorporate measures to remotely lock or unlock doors to provide for limiting travel of individuals within the project. This will create buffer zones to aid responding intervention personnel in reacting to intruders and/or security violators.

- DEFEND – Security planning should lead to a combined system of devices including locks, card readers, and CCTV cameras that provide a mechanism of restricting unauthorized entry.

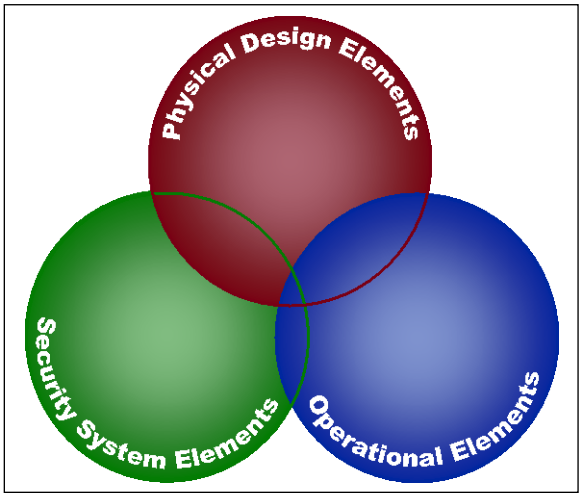
- COMMUNICATE – Security planning should provide the capability for one- and two-way communication at specific locations throughout the facility. The goal of the one-way communication (duress buttons) is to alert the monitoring location that an individual is in need of immediate assistance. The two-way communication (intercoms and assistance stations) allows the monitoring staff to remotely

verify the authority of individuals entering the property after hours without an authorized access card, or to provide assistance as needed to the employees.

The measures used to reach these objectives will be described in this chapter.

The security planning process must balance three key elements to accomplish the security objectives:

1. **Physical Design Elements** – Physical design elements compose the first element in security planning and include physical barriers or elements such as doors, walls, fences, landscaping berms, MEP system design, and structural components. These physical elements, combined with electronic security systems and operational elements, should be used to accomplish the goals of the security plan.



2. **Security System Elements** – The second element in security planning is the security system. The security system complements the physical elements to provide a complete program that provides a safe and secure environment for the users, visitors, and guests. Security systems can be either electronic or mechanical and typically include access control systems, alarm monitoring devices, closed circuit television surveillance

systems, two-way audio communication devices, electrical locking door hardware, and mechanical locking devices. Use these systems where it is necessary to provide a specific level of protection. Do not consider security systems to be a "cure-all" for security. The systems are only one element of the solution.

3 **Operational Elements** – While not discussed in detail in this document, do consider operational elements (personnel, maintenance, operating costs) as the final element of security planning. Carefully consider the consequences of the design and systems elements in relation to the operation of the project once construction is complete and the users occupy the building. Poor security planning will result in increased security operations costs.

PHYSICAL DESIGN ELEMENTS

SITE DEVELOPMENT

- **Evaluate need for controlled access to site**

  Based on the threat level, it may be necessary to control both pedestrian and vehicular access to the site. If so, provide access control points (electric gates with card reader control), or vehicular controls (e.g., barrier arm gates or rolling gates). Consider a guardhouse for prescreening visitors and vehicle inspection.

- **Evaluate location of building entrances**

  Determine if building entrances should be readily visible from campus roadways to facilitate vehicular patrols.

- **Evaluate need for fencing or other perimeter defining elements**

  Define the perimeter of the site to deter unauthorized access. Evaluate landscaping, fencing, or walls to determine whether one (or more) of these elements is warranted to define the site perimeter. If used, design fences that are climb resistant and maintain visibility from the street.

  High-risk environments may also require ram resistant fences.

❑ Evaluate exterior private areas

Design exterior private areas to be easily distinguished from public areas to deter unauthorized access and use of such areas. Consider whether a physical barrier is appropriate to define the private area.

❑ Review proposed building footprint location

In order to mitigate potential damage from adjacent underground systems, consider locating the building footprint as far away as possible from tunnels, subways, manholes, and basements of adjacent properties.

❑ Evaluate need for setbacks

When practical, set the building back from public streets and other adjacent properties to create a buffer that can be controlled and observed by the protection staff and by other physical and electronic means. While setbacks should be site specific based on surroundings and threat profile, we recommend a minimum of 20 feet standoff distance from building envelope for urban sites, 50 feet for controlled vehicles, and 100 feet for non-controlled. Adhering to setback guidelines may reduce or even eliminate the need for hardening of the facility (if needed due to threat level).

- **Evaluate need for vehicular buffers and/or barriers**

  Consider whether it is appropriate to use landscaping buffers or physical barriers, both natural and constructed, to protect the building structure from vehicular damage in the event of an accidental or intentional incident.

  Hardened street furniture such as benches, large urns, or pots are examples of decorative or functional constructed barriers that reduce the potential of vehicular damage to a building. Rock terracing and/or concrete retaining walls can also be effective barriers.

- **Consider the need to restrict vehicular access to pedestrian malls and walkways**

  Review the potential for unauthorized vehicular access in proximity to a building via pedestrian malls and walkways and options for controlling such access.

SITE LIGHTING

- **Review recommended exterior illumination requirements**

  Illuminate the site well for way finding and deterring crime. Make illumination consistent and thorough to prevent dark spots that could be attractive to unauthorized personnel. Make sure to

monitor illuminated areas. A well-lit area may not be secure if it is perceived to be unmonitored.

As a minimum standard, design site lighting levels in accordance with the established recommended levels outlined by the Illuminating Engineering Society of North America (IESNA). Consider increased lighting levels for high-risk site areas.

- **Consider type of light source**

  When selecting and specifying site lighting fixtures, consider that discrepancies in illumination levels and color rendering among the different light fixtures and lamp types can adversely affect the quality of video surveillance. Also, confirm the procurement availability of fixtures selected to meet security design objectives; substitute fixtures may compromise security goals.

- **Evaluate lighting control**

  Determine how the light fixtures will be turned on and off, both for normal operations and for maintenance.

LANDSCAPING

❑ Consider landscaping as a security measure

Consider the use of landscaping as a natural deterrent to crime. Landscaping (trees, heavy shrubbery) can be effective as a vehicular barrier for perimeter protection of a building.

❑ Evaluate mature height of planned landscaping

Keep shrubbery under two feet in height to eliminate potential hiding places and to maintain sight lines. Keep lower tree branches at least 10 feet off of the ground to maintain maximum visibility for pedestrians entering or leaving the building.

UTILITIES

❑ Review and evaluate utility locations

Identify and locate all potential utilities affecting the proposed project in order to mitigate the potential for:

- Service disruption to the building;
- Unauthorized access into the building;
- Their use as a weapon against the property and its occupants.

Review all utilities including:

- Thermal utility tunnels
- Thermal plant
- Electrical substations, generating plant, etc.
- Storm drainage systems
- Sanitary sewerage systems
- Electrical/Communication ductbank
- Utility vault locations
- Overhead utilities, incoming primary electric service
- Pipelines
- Radio/Microwave infrastructure
- Gas lines

PARKING

- **Review illumination requirements for parking areas**

  Review parking areas to ensure they are properly located, illuminated, and situated to provide the appropriate level of security for the visitors, staff, and students while traveling between their vehicles and the building.

As a minimum standard, design parking lighting levels in accordance with the established recommended levels outlined by the Illuminating Engineering Society of North America (IESNA). Consider increased lighting levels in high-risk parking areas.

- **Evaluate the appropriateness of under-building parking**

  Avoid under-building parking whenever possible. Under-building parking greatly increases the potential for building damage due to vehicular incidents. If unavoidable, make provisions to mitigate the increased risk.

- **Evaluate assigned parking requirements**

  Assign parking spaces for visitors, staff, and students. Distribute space using a hierarchical approach, assigning to the most trusted personnel parking closest to the structure. Locate visitor parking in an area that presents little risk to the structure.

- **Evaluate need for highly visible parking areas**

  Site parking areas in locations visible from the building interior; position side parking in areas visible from the street.

- **Evaluate visibility when arranging pedestrian paths between building entrance and parking areas**

  Locate parking, pedestrian pathways, and building entrances in areas that can be observed by as many people as possible to decrease any sense of isolation and increase the sense of safety and well being for visitors, staff, and students.

- **Consider physical separation between building structure and parking structures**

  Separate completely parking areas from the building to reduce the risk of collateral damage in the event of an incident in a parking lot or structure. Consider a minimum separation of 100 feet as a baseline standard. Locate parking areas away from critical facility infrastructure to the greatest extent possible.

EXTERIOR BUILDING CONFIGURATION

- **Evaluate public entrance requirements/ configuration**

  Clearly define public entrances to facilities by walkways and signage. Clearly defined entrances will assist building users and guests to gain entry to the building at the appropriate location. Also consider using architectural elements, lighting, landscaping, and/or paving stones to enhance way finding. Provide access control points for major public entrances for after-hours entry requirements.

Consider whether separate employee and visitor entrances are appropriate.

- **Evaluate non-public entrance requirements/ configuration**

  Clearly mark non-public entrances for the intended user group to reduce the potential for visitors or other unauthorized personnel to enter the building through a restricted or non-public entrance.

- **Consider the need for drop-offs**

  Avoid drop-offs where possible. Where necessary, design drop-offs to accommodate the recommended setback distance to the building exterior.

- **Consider offset entrances and circulation**

  Consider using offset building entrances and circulation corridors rather than straight configured entrances to increase the resistance to attack. If people, mail, or supplies/equipment enter the building before being screened (scanned, x-rayed searched, etc.), isolate the ventilation system of the entry or lobby area in which they await screening from the rest of the building.

  Consider providing airlock (vestibule) at building entrances for external chemical/biological threat.

- **Consider locations of doors and windows**

  Locate windows and doors in areas that enhance building users' visibility of activity on the street, driveway, or common walkway to reduce the

likelihood of unauthorized personnel entering and exiting the building from an obscured location.

- **Evaluate exterior screened-in areas**

  Avoid blind spots or potential hiding areas created by dumpsters, generators, or other exterior elements that require screened enclosures. Consider attaching the screen to the structure to eliminate such areas between the screen and the building.

INTERIOR BUILDING CONFIGURATION

- **Evaluate proposed delivery locations**

  Consider whether to locate the mailroom and loading docks outside of the controlled envelope of building to prevent an incident from affecting the remainder of the building.

  If people, mail, or supplies/equipment enter the building before being screened, isolate the ventilation system of the entry or lobby area in which they await screening from the rest of the building.

- **Evaluate restroom locations**

  Locate restrooms in common areas within major corridors to increase the overall visibility of the entrances to the restrooms.

  Consider including single occupant public restrooms in lobby areas to provide facilities to visitors prior to entering the controlled portion of a building.

- **Evaluate interior circulation areas**

  Do not locate public toilets, service spaces, or access to vertical circulation systems in any non-secure area, including the queuing area before screening at the public entrance.

- **Evaluate location of security office and equipment closets**

  Consider locating the building security office (as applicable) and any major security equipment rooms in the most survivable location of the building to preserve the system operation in the event of an incident. Avoid locating major equipment in lower levels that may be subject to flooding.

- **Evaluate need for personnel screening devices**

  Evaluate the need to include x-ray and magnetometers at pedestrian entrances for high-threat projects.

- **Review lobby configuration**

  Position security and/or reception areas to facilitate screening of all public entrances and any staff entrances that do not benefit from controlled access devices. Consider security posts **at all** entrances for higher threat environments. Review elevator systems, operation, and access.

❑ Evaluate need for segregated circulation

Consider whether segregated circulation corridors for employees and visitors are appropriate based on type of building and threat level.

❑ Consider visibility into corridors

Provide windows and doors with views into hallways to aid in visibility and to reduce concealed space within a building.

❑ Evaluate stairwell accessibility

Control access to roof areas and/or basements through stairwells to restrict traffic to only those persons authorized to access these areas.

If stairs are to be used for floor-to-floor travel, consider excluding stairs from the controlled envelope of the building. To limit travel to specific floors, place access control devices within the stairwells.

❑ Evaluate loading dock requirements

Consider placing loading dock outside the controlled envelope of the building to prevent delivery personnel from gaining access to the building interior. When feasible, locate dock away from populated areas. Consider options for reducing the entry of contaminants into occupied portions of the building from the loading dock.

❑ **Evaluate interior lighting**

As a minimum standard, design interior lighting levels in accordance with the established recommended levels as outlined by the Illuminating Engineering Society of North America (IESNA). Consider increased lighting levels in high-risk areas.

❑ **Evaluate door hardware and locking mechanisms**

Evaluate the type of door hardware specified for coordination with other security provisions, including security systems discussed later in this chapter.

STRUCTURAL CONSIDERATIONS

In the effort to protect a structure, Structural Blast Hardening is the last resort; always regard detection and prevention as the first line of defense.

General Considerations for all Structures

Building collapse is the primary contributing factor to death from terrorist bombings, while flying glass is the primary source of injury from terrorist bombings.

❑ **Evaluate structural system blast resistance**

Backpack size bombs typically do not put primary structural systems at risk. Therefore, focus structural system blast resistance on vehicle trunk-sized bombs and larger.

❑ Review standoff distances

Standoff distance is critical. Blast effects on a structural member are generally a function of distance to the third power. For example: a bomb placed 10 feet from a column will have eight times the effect on that individual column versus the same bomb placed 20 feet from the column. $(20 \text{ ft.}/10 \text{ ft.})^3$ equals eight times the local blast effect on the column.

❑ Evaluate confined spaces

Avoid under-building parking structures open to the public. Standoff distances cannot be limited. Blast pressures are more likely to be confined. Confined blasts will dramatically magnify the blast effects on the whole structural system due to quasi-static gas pressure loads.

Avoid access to confined space by public vehicles. In confined spaces into which public vehicles must be allowed, provide blast venting to reduce the quasi-static gas pressure loads.

❑ Review structural concepts

Avoid the use of transfer girders. One column failure at a lower level could bring down three or more columns above the transfer girder.

Unique Considerations for High-Risk Structures

We recommend a blast consultant join the project team in the earliest programming stages of a high-risk project. The blast consultant will then need to be part of the A/E project team through the entire design process. Here are some basic and simplified design issues that the blast consultant will consider for the structural design.

- **Evaluate building exterior construction**

  Determine the need to provide a blast-resistant building exterior or "skin". Consider blast-resistant exteriors or curtain-wall systems for high-risk structures, particularly designs that dissipate forces from explosions.

- **Review potential for progressive failure**

  The blast consultant will make recommendations to help prevent progressive failure of the structure. Example: The failure of a single column at a lower level could lead to the collapse of the entire structure above it and/or around it.

- **Evaluate Structural Redundancy**

  Evaluate the need to increase redundancy in the structural design. Example: Add negative moment reinforcing to concrete beams that are designed as simply supported beams; such reinforcement could prevent the catastrophic collapse of a beam that is severely damaged at mid-span.

- **Consider load reversal**

  Blasts may induce uplift on beams that are normally designed for simple gravity loading. Minimize the effects of these load reversals with additional rebar for concrete structures and additional connection detailing in steel.

- **Evaluate ductility**

  Increase the ductility in a system through design. Increased ductility will help the structure to deform (absorb energy) without catastrophic failure. Seismic Zone detailing goes a long way towards this goal. Example: Make sure that shear strength exceeds flexural strength in the at-risk beams.

- **Consider round beams**

  Round columns are more blast resistant than square columns. Round concrete columns may include additional spiral reinforcing or an external steel pipe jacket. Round steel columns may be filled with grout.

MEP CONSIDERATIONS

Traditionally, security planners have paid little attention to the mechanical, electrical, and plumbing (MEP) systems design on the "typical" commercial or institutional project. They expected that compliance with reasonable safety and health requirements established by building codes and standards was sufficient. In the wake of the September 11th attack, this

presumption is being reevaluated. MEP systems must now be reviewed and evaluated to deter tampering and compromise from both internal and external sources. Designers are encouraged to recognize that building codes are minimum requirements and that, when the project threat level requires it, design in "excess of code" is desirable and has demonstrated benefits against extraordinary incidents.

The MEP system recommendations we provide below focus on the many aspects of building performance that affect the health and safety of the occupants under extraordinary incidents. However, these recommendations are not unrelated to those recommended for accidental and naturally occurring incidences, such as flooding and fires. Consequently, it is useful to distinguish between those that are "unique" to extraordinary incidents and those that are embodied within the "general considerations" recommendations of professional engineers.

We have prepared the following information to provide project teams with additional guidelines on the design of MEP systems.

MECHANICAL (HVAC) SYSTEMS

General Considerations

- **Review outside air intake location**

  Place intakes at the highest practical level on the building; cover intakes with screens so that objects

cannot be tossed into the intakes, and slope the screens so objects thrown onto the screen roll or slide off, away from the intake.

- **Review rooftop equipment locations**

  Locate rooftop equipment away from the roof's edge to deter tampering.

- **Evaluate building air exhaust locations**

  Use central exhausts that combine flows from many collecting stations where safe and practical. By combining several exhaust streams, central systems dilute intermittent bursts of contamination from a single station. Also, the combined flow forms an exhaust plume that rises a greater distance above the emitting building.

  In some cases, separate exhaust systems are mandatory. In these cases, group separate exhaust stacks in a tight cluster to take advantage of the larger plume rise of the resulting combined jet.

  If exhaust is discharged from several locations on a roof, site intakes to minimize contamination.

  Air exhausted from laboratory hoods and special exhaust systems will be discharged above the roof at a location, height, and velocity sufficient to prevent re-entrainment or re-entry of chemicals and to prevent exposures to personnel.

  Consider also the effect of building exhaust on adjacent and/or adjoining buildings.

❑ Evaluate building pressure requirements

Maintain continuous building pressure control and require air ducts to be as tight as practical. Building pressurization requires that the air exchange that normally occurs due to wind pressure, chimney effect, and operation of fans be reduced to zero. To achieve this:

- Close dampers to tighten the building shell in transitioning to the protective mode, and
- Introduce filtered air at a rate sufficient to produce an overpressure in the building and create an outward flow through all cracks, pores, seams, and other openings in the building shell.

It is also important to note that building pressurization can impact the ability of door closures to close and latch doors. Consider the need to close and latch exterior doors consistently and reliably.

❑ Consider securing access to mechanical spaces

Restrict access to mechanical spaces with either high security mechanical locking devices or electronic access control devices.

❑ **Consider providing a single point for disconnecting utilities** 5/15/03

Provide a single consolidated location for disconnecting or shutting-off critical utilities, such as natural gas and electrical supplies to the building. The location should be the most secure, not just the most convenient, and the shut-off points should be clearly identified and readily available to the fire responders to an extraordinary event, but not to intruders.

Unique Considerations

❑ **Evaluate need for space ventilation**

Supply a constant volume of ventilation air to each zone within the building at a rate that complies with ASHRAE Standard 62-1999. Connect the ventilation fan systems to the standby power that supports critical and life safety systems.

❑ **Consider improved filtration of supply air**

Minimize bypass of particulate contaminants around air filters by ensuring that filter-to-filter rack and filter-to-filter seals are in place, and that there are not any air leaks in the air handling cabinet between the filter rack and supply fan.

Verify that filter efficiency has been upgraded to the highest Minimum Efficiency Reporting Value (MERV) attainable under existing conditions of space and available airflow capacity.

Increase fan size and power requirements to accommodate additional filtration. Consider an analysis of the emergency power capacity if these systems will be placed on emergency power.

- ❑ **Evaluate incorporation of protective logic with Building Automation System** 5/15/03

  Verify that all fire protection and life safety systems receive the highest priority within any automated building or energy management system. To accomplish this, provide a Controls Points List and define a Sequence of Operation confirming that this priority has been implemented in the design. The Sequence of Operation should implement the following HVAC response:

  - **Emergency Systems Shut-down**
    For buildings without specific unique protective features, consider an alternative control sequence in which the HVAC systems shut down in response to an attack.
  - **Emergency Systems Operations**
    For buildings designed with specific unique protective features, transfer from normal to emergency mode of operation will depend upon both the agent and the point of release.
    1. For an internal release, the HVAC system should respond to a manual or automatic signal by isolating the zone of release, impeding the CBR agent from directly migrating or

being transported to other zones, and removing the agent with the filtration/air cleaning components of the HVAC system.

2. For an external release, the HVAC system, if provided with high performance filtration effective for that agent, should continue to run.

❑ **Evaluate need for specialized HVAC equipment**

In high-risk facilities, consider utilizing specialized HVAC system equipment such as UV systems within air handlers designed to kill certain biological agents.

❑ **Consider the need for compartmentalization and areas of refuge** 5/15/03

In large high-risk facilities, consider the need for additional compartmentalization both horizontally and vertically, compared to that for fire and life-safety requirements. Design and construct the compartments to provide fire, smoke, and particulate separation. This system of compartmentalization, with no cross contamination of return air, can minimize the area of dispersion from the internal release of a biological or radiological agent and provide some short-term protection from the spread of a chemical agent.

PLUMBING SYSTEMS

- **Evaluate need for protection of domestic water supply**

  Secure manhole covers that access the water source with tamper resistant fastening devices to protect domestic water supplies from tampering, such as the introduction of a foreign substance into the water supply.

- **Consider securing access to plumbing systems and spaces**

  Restrict access to areas with plumbing systems, including mechanical rooms and utility tunnels, with either high security mechanical locking devices or electronic access control devices.

ELECTRICAL SYSTEMS

- **Determine need to provide isolated/redundant incoming electrical service feeds**

  Review the project requirements for highly reliable incoming power service feeds. If redundant feeds are necessary, they should enter the facility from geographically separate areas.

- **Evaluate need to protect incoming electrical service**

  Protect the incoming service feed from vandalism and sabotage.

- **Evaluate need for emergency power source**

  Consider whether a backup power source is needed or required. Ensure the backup electrical systems are designed as separate services (widely separated electrically and physically).

- **Consider restricting access to inside power distribution and emergency power generation areas**

  Restrict access to the power distribution areas within the building, allowing only authorized personnel to gain entry.

- **Evaluate survivability of service feed and power distribution locations**

  Determine which threats are most likely to affect the power reliability and implement the appropriate mitigation steps for both incoming service feeds and interior distribution. For example, in areas prone to flood, either locate power distribution above the recognized flood plain high water mark or provide an adequate level of waterproofing to electrical rooms.

- **Evaluate survivability of life safety systems**

  Determine which threats are most likely to affect the life safety systems for the facility and implement appropriate mitigation measures. Consider distributed fire alarm systems in which individual

panels remain operational in the event that the rest of the system is destroyed or damaged.

- **Consider redundant interior power distribution**

  Determine whether redundant or highly reliable distribution systems are required to maintain electric service within the building for life safety, security, and other critical systems.

- **Consider supplemental evacuation annunciation systems for high-risk projects**

  Consider the need for a supplemental evacuation notification and way finding system for high-risk environments in the event life safety systems do not activate during an incident.

COMMISSIONING OF MEP SYSTEMS

5/15/03

All measures used to decrease building vulnerability, including proper operation of the mechanical, electrical, and life-safety systems of the building under both normal operation and extraordinary incidents, shall be tested as a part of a building commissioning process. The commissioning process ensures that systems are designed, installed, functionally tested and operated in conformity with the design intent.

TELECOMMUNICATION SYSTEMS

- **Evaluate need for highly reliable telecom and data systems**

  Determine the requirements for the telecom and data systems and provide redundant and geographically separate infrastructure systems as necessary. Consider wiring communication systems in a loop configuration to enhance survivability of the systems. Maintain all systems in a condition that allows easy inspection for validation/verification.

SECURITY SYSTEMS ELEMENTS

The security systems form the second key element in the creation of the overall security plan. After proper development of the physical design elements, the security systems provide the necessary controls and monitoring of the building to ensure a safe and secure environment for visitors, students, and staff. The electronic systems requirements of any project will depend greatly on each campus' existing security system capabilities and the system philosophy currently employed. Security systems play a major role in completing the planning process. In planning the security systems, the project team will:

- **Determine need for outside assistance**

  Evaluate the need for an outside consultant to provide assistance in planning and engineering the security system requirements for a project. We encourage the project team to seek outside professional assistance to work with the team to determine the project requirements and to properly engineer the system.

- **Review existing campus security capabilities and policies**

  Review existing campus security capabilities to determine if the current systems can be expanded to incorporate the new project. The capabilities of the

existing systems will guide the team in determining the requirements for the project security systems.

- **Determine the requirement for local 24 hour security presence**

  Review the requirements for a local security staff presence. Determine if the project will require a 24-hour, seven-days-a-week local security presence, a presence during business hours only, or no presence at all. If there is a 24-hour security staff within the building, determine what its responsibilities will be.

- **Determine the need and capability for local monitoring and control vs. centralized monitoring and control**

  Determine the capabilities of the campus police department to monitor security alarms. Consider whether to configure the building to support local (inside the building) monitoring and control or to authorize the campus police department to monitor and control the system.

  Note: As a general rule, either the campus police department or a remote commercial Central Monitoring facility should monitor all electronic systems.

- **Determine the extent to which system flexibility will be required**

  Consider the incorporation of flexible design parameters to accommodate future system changes

in building usage and/or internal renovations consistent with the dynamic nature of educational institutions.

- **Evaluate survivability of security equipment rooms and central monitoring locations**

  Determine which threats are most likely to affect system reliability and implement the appropriate mitigation steps. For example, in areas prone to flood, either locate security system distribution equipment rooms above the recognized flood plain high water mark or provide an adequate level of waterproofing to equipment rooms. Locate critical security infrastructure in the core, or most survivable location within the facility.

- **Commissioning of security systems**

  In high-risk facilities, conduct a formal commissioning process for the security systems, including pushing systems to operational limits ("fail" testing), to confirm they are operating in accordance with the design intent.

After addressing the above considerations, move into the planning of the individual security system components.

ACCESS CONTROL SYSTEM

- **An access control system restricts access to a building or an interior area in a building. In determining the need for an access control system, the project team will: Evaluate the need for restricted access to the site**

  Determine whether the project threat level requires restricted access to the site.

- **Evaluate the need for restricted access to the building entrances**

  Evaluate the need to control access to all building entrances, public-only entrances, or staff entrances, based on the building type and threat level.

- **Evaluate the need for restricted access to critical interior areas and/or rooms**

  Determine the need to restrict and control access into sensitive or critical function areas. Also consider the need to control access from areas like mailrooms, loading docks, and visitor lobbies.

- **Determine the hours of access**

  Determine the hours of operation of the facility and when users will require access to the site or building.

- **Consider the audit trail requirements of the project**

  Consider providing access control devices on areas where an audit trail (history log) of all persons entering and leaving an area would be beneficial to the project. Provide a minimum of six (6) months of activity on-line with permanent archiving of the history log.

- **Review Electric Locking Hardware**

  Design electric locking hardware with an emphasis on using electromechanical, **fail-secure** hardware wherever possible.

  Electromechanical hardware provides one-direction electric control with a mechanical means of egress. Locks of this type do not inhibit a person's ability to exit the controlled space regardless of the operability of the electrified portion of the lock.

  Fail-secure hardware provides a higher degree of control, i.e., if a power failure occurs, the lock fails in the locked position, rather than in the unlocked position. Assess each controlled door to determine whether the building codes and local Authority Having Jurisdiction (AHJ) will permit fail-secure locks in a given location.

  Give additional consideration to selecting locking hardware that will consistently and reliably close and latch the door, based on the door's weight, size, and hinge design. Also consider heavy-duty door

closers to overcome building pressurization problems.

INTRUSION DETECTION AND ALARM MONITORING (IDAMS)

The intrusion detection and alarm monitoring system detects unauthorized entry attempts into the building and transmits an alarm signal to the appropriate authorities, e.g., the local security office, the campus police department, or a private security monitoring company—depending on the campus' capabilities. In planning the IDAMS, the project team will:

- **Determine the need for intrusion detection and alarm monitoring**

  Most buildings require at least a basic level of alarm monitoring to detect unauthorized persons attempting to gain access. If a building is open to the public 24 hours a day, such as a medical center, student center, or public safety building, use building occupancy periods to direct the IDAMS requirements. While such buildings may always be open, often there are either non-public entrances or interior areas requiring intrusion detection alarms.

- **Determine need for personnel alarms**

  Review the requirements to provide personnel duress alarms in key areas to provide the building users with the ability to signal for assistance in the event of an emergency.

EMERGENCY ASSISTANCE COMMUNICATIONS

Emergency assistance communications systems provide building users with the ability to signal a need for assistance. These devices are typically located within parking structures near stairwells and elevator lobbies. They can also be used on major pedestrian paths. In evaluating the need for emergency communication stations, the project team will:

- **Review campus policies regarding emergency assistance stations**

  Determine whether these devices have been used previously on campus and whether the threat profile exposes the need for such protection.

- **Review pedestrian access from and within parking structures and surface lots**

  Evaluate the need to provide devices within parking structures at stairwells and elevator lobbies, in surface parking lots, and along pedestrian pathways around the building.

- **Determine monitoring capability of local campus**

  Determine the monitoring location of the emergency assistance stations. This location can be either the campus police department or the building itself, if a local 24-hour security office is continuously staffed.

CLOSED CIRCUIT TELEVISION SURVEILLANCE SYSTEM

A closed circuit television surveillance system (CCTV) enables the security staff to monitor more locations than it has the ability to physically staff. It can also record certain areas on a continuous basis for evidentiary purposes. Most buildings will require a CCTV system. In order to determine the general requirements of the CCTV system, the project team should:

- **Review high risk areas in and around the building**

  Review the site and building exterior to determine the need to place CCTV devices along the major traffic arteries for both vehicular and pedestrian monitoring.

- **Review building entrances configurations**

  Review the building entrances to determine the need to place CCTV devices outside the building to monitor the exterior entrances. Consider placing cameras inside the building lobbies to monitor visitor traffic and non-staffed entrances.

- **Evaluate sensitive and critical interior locations**

  Review interior building areas where video surveillance is required. Evaluate interior areas based on sensitivity of the area, criticality of information or data within the area, and the value of the equipment housed in the area.

- **Determine monitoring methodology and location**

  Review the monitoring methodology to determine the requirements of the local police/security staff. A locally monitored system may be appropriate if the building has a 24-hour security office. If the campus police have the capability and desire to monitor individual buildings, offsite monitoring may be preferable.

- **Determine video recording requirements**

  The CCTV system records activity. All cameras record on a continuous basis. Determine whether the recording location will be within the building or in a remote location, possibly at the police department.

OPERATIONAL ELEMENTS

Operational elements, the third component of a security plan, are crucial to the success of the plan. This document does not provide detailed recommendations regarding operational elements. The local campus police department, Environmental Health and Safety (EH&S) department, facilities department, and the various building user groups will develop the operational procedures for a project once the physical design elements and security systems have been developed.

Every building management team will have a preparedness plan to follow in the event of an extraordinary incident. Assign a key member of the management team to safeguard the plan; the plan will be written, documented, and kept prominently in the building files.

The following three recommendations can assist building owners and managers in providing the maximum protection available against various levels of risk:

- Understand the capabilities of your building and its systems;
- Ensure that your building is performing as intended; and
- Do not make changes to building performance unless the consequences are understood.

Chapter Review

Upon completion of the security planning process, you will have defined solutions to the security threats identified during the security assessment.

Solutions will involve both the physical design elements and the electronic system needs for the project. Don't overlook the impact on operations that the solutions you implement will have; everything you've designed will have some consequence on the operation of the building or the campus security staff, whether from a manpower or systems perspective.

a Appendices

a1 Acknowledgments

Office of Facilities Planning and Construction Task Force
The University of Texas System

Mr. Bob Rawski, Senior Project Manager, Austin, Chair
Ms. Carol Bowman, P.E., Electrical Engineer
Mr. Richard De Leon, Senior Project Manager, South Texas
Mr. Jim Hicks, Senior Project Manager, Houston
Mr. Charles Kieffer, P.E., Mechanical Engineer
Mr. John Peterson, P.E., Mechanical Engineer
Mr. Michael Petty, Senior Project Manager, Galveston and Tyler
Mr. Jerry Salcher, P.E., Senior Project Manager, North and West Texas
Mr. J.B. White, Structural Engineer-in-Training

Campus Advisory Group

Ms. Vickie Noble, P.E., Director, Engineering Services
The University of Texas Health Center at Tyler

Mr. Dan Pena, Assistant Chief of Police
The University of Texas at San Antonio

Mr. Craig Powell, CHMM, Director, EH&S
The University of Texas at Arlington

Mr. Charlie Price, Chief of Police
The University of Texas M. D. Anderson Cancer Center and
The University of Texas Health Science Center at Houston

Mr. David Rea, Manager, Capital Projects
The University of Texas at Austin

Consultants

Mr. Mickey Walling, CPP, Managing Associate, Kroll Schiff & Associates
Ms. Debra Packard, Communications Specialist, OFPC, The University of Texas System

a2 References

THE FOLLOWING SOURCES WERE USED IN THE PREPARATION OF THIS DOCUMENT:

- American Institute of Architects (AIA). *Building Security Through Design Virtual Conference.* American Institute of Architects. November 5, 2001.

- American Society of Heating, Refrigeration, and Air Conditioning Engineers, Inc. (ASHRAE). *ASHRAE Handbook: HVAC Applications.* Chapter 43. American Society of Heating, Refrigeration, and Air Conditioning Engineers, Inc. 1999.

- American Society of Heating, Refrigeration, and Air Conditioning Engineers, Inc. (ASHRAE). *ASHRAE Standard 62-1999, Ventilation for Acceptable Indoor Air Quality.* American Society of Heating, Refrigeration, and Air Conditioning Engineers, Inc. 1999.

- American Society of Heating, Refrigeration, and Air Conditioning Engineers, Inc. (ASHRAE), Presidential Study Group on Health and Safety Under Extraordinary Incidents. *Risk Management Guidance for Health and Safety Under Extraordinary Incidents.* American Society of Heating, Refrigeration, and Air Conditioning Engineers, Inc. January 12, 2002.

- Baker, Wilfred Engineering, Inc.; FKP Architects, Inc.; Moore, Walter P. Engineers and Consultants; U. T. System OFPC. Meeting with representatives to discuss general blast design considerations for a large U. T. System project. Austin, TX: January 25, 2002.

- Bordenaro, Michael. *Backup Facilities Break Free From a Black-box Approach*. Engineering News-Record. September 23, 2002.

- Carrigan, James. *Survival Strategies for Fire Alarm Systems*. Building Operating Management. October 2002.

- Crowe, Timothy D. *Crime Prevention Through Environmental Design*. National Crime Prevention Institute. 1991.

- Ettouney, Mohammed, P.E.; Smilowitz, Robert, P.E.; and Rittenhouse, Tod, P.E. *Blast Resistance Design of Commercial Buildings.* Weidlinger Associates website. www.wai.com. 2002.

- Federal Reserve System. *Federal Reserve System Facility & Security Design Guidelines: Minimum Design Criteria for Security and Construction.* Washington, DC: Federal Reserve System. September 2001.

- Hitchings, Leah. *High-tech Protection Moves From Lab to Marketplace*. Engineering News-Record. September 23, 2002.

- Kozlowksi, David. *HVAC Systems Can Be Facilities' Achilles Heel*. Building Operating Management. October 2002.

- Linn, Charles. *These Shining Examples Heighten Building Safety*. Engineering News-Record. September 23, 2002.

- Maas, Angela. *Parking Structures Add Guards, Limit Access*. Building Operating Management. October 2002.

- Massa, Ronald J., PhD. *Blast Design Consulting: A New Design Team Function.* RJA Group website. www.rjagroup.com. 2002.

- Murdoch, J.; Harold, R.; Goldsbury, C. J., Editors. *IESNA Lighting Ready Reference: Recommended Illuminations Levels.* Illuminating Engineering Society of North America. 1996.

- National Institutes of Building Sciences. *Whole Building Design Guide.* National Institutes of Building Sciences website. 2002.

- National Research Council of the National Academy of Sciences and the National Academy of Engineering. *Protecting People and Buildings from Terrorism: Technology*

Transfer for Blast Effects Mitigation. Washington, DC: National Academy Press. November 2001.

- National Fire Protection Association. *NFPA 45: Standards on Fire Protection for Laboratories Using Chemicals.* Chapter 6, 2000 Edition. Quincy, MA: National Fire Protection Association. 2000.

- Prendergast, John. *Oklahoma City Aftermath.* October 1995.

- Rittenhouse, Tod. *Designing Terrorist Resistant Buildings: Fire Engineering.*

- U. S. Army Corps of Engineers, Engineering and Construction Division. *Protecting Buildings And Their Occupants From Airborne Hazards, TI853-0.* Washington, DC: U.S. Army Corps of Engineers. October 2001.

- United States Department of Justice. *ISC Security Design Criteria for New Federal Office Buildings and Major Modernization Projects: United States Department of Justice Interagency Security Committee Report.* Washington, DC: United States Department of Justice. September 30, 1998.

- Weidlinger Associates. *Structural Engineers Combat Terrorism.* Weidlinger Associates website newsletter. Volume 9, Number 1. Spring 1996. www.wai.com.

a3 Resources For Additional Information

ADDITIONAL INFORMATION REGARDING THE RECOMMENDATIONS CAN BE OBTAINED FROM THE FOLLOWING SOURCES:

ARCHITECTURAL

American Institute of Architects (AIA) Building Security Through Design	http://www.aia.org/security/
Whole Building Design Guide	http://www.wbdg.org
Gensler Architecture, Design and Planning Worldwide: Security & Openness: Integrating Security into Office Buildings	http://www.gensler.com/events/index.htm
Architectural Record, AIA, RTKL, National Building Museum, and Urban Land Institute	http://www.archrecord.com/news/articles/nbm112101.asp
"Freedom without Fortresses? Shaping the New Secure Environment" (Symposium)	http://www.rtkl.com/id4/symposium.asp#talk
American Society of Landscape Architects Security Design Coalition	http://www.asla.org/members/publicaffairs/factsheet/securedesignfs.htm
Jane's Facility Security Handbook, Texas Department of Public Safety	http://www.txdps.state.tx.us

MECHANICAL, ELECTRICAL & PLUMBING

American Society of Heating, Refrigeration and Air-Conditioning Engineers	http://www.ashrae.org
National Fire Protection Association – NFPA 45, 2000 Edition	http://www.nfpa.org
Illuminating Engineering Society of North America (IESNA)	http://www.iesna.org

Institute of Electrical and Electronics Engineers, Inc. (IEEE)	http://www.ieee.org
National Academy of Sciences	http://www.nationalacademies.org

STRUCTURAL

U.S. Army Corps of Engineers	http://www.usace.army.mil

SECURITY DESIGN

Crime Prevention Through Environmental Design (CPTED)	http://.www.cpted.net

GOVERNMENTAL

Centers for Disease Control (CDC) (5/15/03)	http://www.cdc.gov
General Services Administration (GSA)	http://www.hydra.gsa.gov/pbs/firstimpressions/
National Capital Planning Commission (NCPC)	http://www.ncpc.gov/planning.html
National Science Foundation	http://www.nsf.gov/homepage/programs/eng.htm
U.S. Army Corps of Engineers	http://www.usace.army.mil